MATHEMATICS OF COMPUTATION
VOLUME 60, NUMBER 202
APRIL 1993, PAGES 811–816

SMALL TWO-VARIABLE EXPONENTIAL DIOPHANTINE EQUATIONS

ROBERT STYER

ABSTRACT. We examine exponential Diophantine equations of the form $ab^x = cd^y + e$. Consider $a \leq 50$, $c \leq 50$, $|e| \leq 1000$, and b and d from the set of primes 2, 3, 5, 7, 11, and 13. Our work proves that no equation with parameters in these ranges can have solutions with $x > 18$. Our algorithm formalizes and extends a method used by Guy, Lacampagne, and Selfridge in 1987.

INTRODUCTION

While investigating a problem of Katai, the author [6] needed all solutions to hundreds of equations of the form $ab^x = cd^y + e$, where b and d are small primes and the a, c, and e are reasonably small. This paper outlines an efficient method to examine many such equations and to prove that none have large solutions. When b and d are primes up to 13, when $a \leq 50$ and $c \leq 50$, and when $|e| \leq 1000$, our work shows that no equation of the form $ab^x = cd^y + e$ has a solution with $x > 18$.

When finding solutions to equations of the form $ab^x = cd^y + e$, one can quickly and easily try all small values for x and y, say, up to 100. Our problem, of course, is to prove there are no larger solutions.

This problem is deterministic, as one may see by using Baker's [1] estimates of logarithmic sums. B. M. M. De Weger [3] has combined Baker's work with his version of the L^3 Basis Reduction Algorithm to solve a vast array of similar equations. Our goal, however, is to use straightforward congruential relations to solve these equations; in particular, we will expand upon a simple method noticed by Guy, Lacampagne, and Selfridge.

Guy, Lacampagne, and Selfridge [4] use a curious method with equations such as $5 = 2^x - 3^y$. They begin with a known solution $x = 5$ and $y = 3$. Then they rearrange and factor to get $(2^a - 1)2^5 = (3^b - 1)3^3$, where $a = x - 5$ and $b = y - 3$. Since 27 divides $2^a - 1$ but 81 does not, $a \equiv 0 \bmod 9$ but $a \not\equiv 0 \bmod 27$. This is the first crucial step. The next step is to bootstrap ourselves until we reach a contradiction. Since 32 divides $3^b - 1$, $b \equiv 0 \bmod 8$. Then $41|3^8 - 1$, so $41|2^a - 1$, consequently, $a \equiv 0 \bmod 20$. Similarly, $11|2^{20} - 1$, so $11|3^b - 1$ and hence $b \equiv 0 \bmod 5$. $7|2^3 - 1$, so $7|3^b - 1$, so $b \equiv 0 \bmod 6$. Now $271|3^{30} - 1$, so $271|2^a - 1$. Therefore, $a \equiv 0 \bmod 135$, but then $a \equiv 0 \bmod 27$, which is a contradiction, proving that there are no larger solutions.

Received by the editor July 3, 1991 and, in revised form, February 18, 1992.
1991 *Mathematics Subject Classification.* Primary 11D61.

This approach has two flaws. First, it requires that we know one solution. (By a recent result of Reese Scott [5], for equations of the form $p^m + c = q^n$, the existence of one solution is often sufficient to prove that there are no others.) Second, this method looks rather haphazardly for suitable factorizations. Our goal is to remove these deficiencies.

1. Some examples with $b = 3$ and $d = 7$

A typical equation might be $5 \cdot 3^x = 2 \cdot 7^y - 23$. Suppose that this equation had positive integer solutions for x and y with $x \geq 3$. Then we might view this equation mod 3^3, which shows that

$$0 \equiv 2 \cdot 7^y - 23 \bmod 27,$$

and so we can solve for y. One finds $y \equiv 4 \bmod 9$, since 7 has period 9 modulo 27. We now have

$$5 \cdot 3^x = 2 \cdot 7^{4+9m} - 23$$

for some integer m.

We now observe that 19 and 37 divide $7^9 - 1$, so $7^9 \equiv 1 \bmod 19$ and $7^9 \equiv 1 \bmod 37$. Thus, our equation becomes

$$5 \cdot 3^x \equiv 2 \cdot 7^4 - 23 \bmod 19$$

and similarly modulo 37. We can now solve for x, up to the period of 3 modulo 19 (which happens to be 18). One finds that $x \equiv 14 \bmod 18$.

Now consider the equation modulo 37. Again, one can solve for x up to the period of 3 modulo 37 (which also happens to be 18). But now one calculates that $x \equiv 7 \bmod 18$. Since x cannot be both 14 and 7 modulo 18, we have reached a contradiction, which proves that there cannot be any solution with $x \geq 3$. (It is easy to see there are no lower solutions.)

As a second example, consider the equation $2 \cdot 3^x = 5 \cdot 7^y + 19$. One can find a solution $x = 3$ and $y = 1$. So we assume a solution with $x \geq 4$. If we view this equation modulo 3^4, we can solve

$$0 \equiv 5 \cdot 7^y + 19 \bmod 81$$

for y to get $y \equiv 10 \bmod 27$. Our equation is now

$$2 \cdot 3^x = 5 \cdot 7^{10+27m} + 19$$

for some m.

We saw that 19 and 37 divide $7^9 - 1$, which divides $7^{27} - 1$. Similar to the last example, we may view this equation modulo 19 and find that $x \equiv 3 \bmod 18$. If we consider this equation modulo 37, one also finds $x \equiv 3 \bmod 18$. One might have expected this, since $x = 3$ and $y = 1$ is a solution.

Using [2], we note that 109 divides $7^{27} - 1$, so $7^{27} \equiv 1 \bmod 109$. Then

$$2 \cdot 3^x \equiv 5 \cdot 7^{10} + 19 \bmod 109$$

and so we can solve for x. One finds $x \equiv 11 \bmod 27$. This gives the desired contradiction, since when we view the equation modulo 37, $x \equiv 3 \bmod 9$, but when we view it modulo 109, $x \equiv 2 \bmod 9$. The contradiction proves that there are no solutions with $x \geq 4$.

For a third example, consider the equation $29 \cdot 3^x = 34 \cdot 7^y - 631$ which has a solution $x = 9$ and $y = 5$. Assume it has a solution with $x \geq 10$. If one

views the equation modulo 3^9, one gets $y \equiv 5 \bmod 3^8$. When we calculate x, we see that $x \equiv 0 \bmod 9$ modulo any of the primes 19, 37, or 109.

But now consider the equation modulo 3^{10}. One finds that $y \equiv 13127 \bmod 3^9$. We will use the prime 39367, which divides $7^{3^9}-1$. The period of 3 modulo 39367 is 39366 which is divisible by 9. We consider the equation modulo 39367 to find that $x \equiv 1 \bmod 9$ (for speed in computation, it is easier not to compute $x \equiv 6652 \bmod 39366$). But this contradicts the value of x obtained when we used the primes 19, 37, and 109, hence we have shown there are no solutions with $x \geq 10$.

Often much less calculation is needed to find a contradiction. For example, consider $2 \cdot 3^x = 5 \cdot 7^y + 11$. If we consider this equation modulo 3 we find no possible value for y, which proves that the equation has no solutions with $x \geq 1$. A second example is the equation $2 \cdot 3^x = 5 \cdot 7^y + 13$. Viewing this modulo 3^3 one finds $y \equiv 3 \bmod 9$. If one considers $2 \cdot 3^x \equiv 5 \cdot 7^3 + 13 \bmod 37$, one finds that there is no possible value for x, hence this equation can have no solution with $x \geq 3$.

Our goal is to examine millions of equations of the form $ab^x = cd^y + e$. The proposed algorithm will first fix the b and d, then preprocess as much as possible before considering the a, c, and e parameters. For each equation in our range of parameters, we will look for a contradiction which proves that the equation can have no large solutions. In practice it takes very little calculation to find a suitable contradiction, so we are able to check large numbers of equations.

2. The algorithm

Fix coprime b and d. We begin by preprocessing whatever will involve only the b and d. We will note in our algorithm where we employ the preprocessed information, and will discuss later the details of the preprocessing.

One then chooses values for the parameters a, c, and e. Consider one of these equations $ab^x = cd^y + e$. Assume that we are only interested in equations with solutions $x \geq h$. View the equation $ab^x = cd^y + e$ modulo b^h. Let β be the period of d modulo b^h, so $d^\beta \equiv 1 \bmod b^h$. (We would know β from our preprocessing.)

Find the value for y, say y_0, such that $cd^{y_0} + e \equiv 0 \bmod b^h$. Often no such y exists, which contradicts the assumption that the equation has a solution with $x \geq h$. If there is a solution with $x \geq h$, then y must satisfy $y \equiv y_0 \bmod \beta$. Consider any reasonably small prime p which divides $d^\beta - 1$ with $(ab, p) = 1$. (In our preprocessing step, we found this set of primes p.) Then $d^\beta \equiv 1 \bmod p$.

Now

$$ab^x \equiv cd^{y_0 + m\beta} + e \pmod{p},$$
$$ab^x \equiv cd^{y_0} + e \pmod{p}.$$

For each prime p in our set, we could now find a value for x, call it x_p, so the left side equals the right side. There may not be any value for x which again contradicts the assumption that there is a solution with $x \geq h$. If there is a solution $x \geq h$, then $x_p \equiv x \bmod \pi(b, p)$, where $\pi(b, p)$ is the period of b modulo the prime p. (This period was found in the preprocessing step.) But suppose we find two of our primes p_1 and p_2 such that

$$x_{p_1} \not\equiv x_{p_2} \bmod \text{g. c. d.}\,(\pi(b, p_1), \pi(b, p_2)).$$

This contradiction would prove that the equation has no solution with $x \geq h$. Crucial observation: If there is a solution $x \geq h$, then for each of our primes p, $x_p \equiv x \bmod \pi(b, p)$. If there is no solution to $ab^x = cd^y + e$ with $x \geq h$, then when a value of x_p exists, it seems to be somewhat arbitrary modulo $\pi(b, p)$.

Given our crucial observation, and the fact that the values of the $\pi(b, p)$ tend to have common factors, one need only calculate a few x_p until one finds primes whose x-values are inconsistent. Thus, in practice it seems to take very little calculation to find a contradiction, which would prove the equation has no solutions with $x \geq h$. We thus can check large ranges of values for a, c, and e.

When $b = 2$, the procedure is easier because of Fermat primes. View $a \cdot 2^x = cd^y + e$ modulo 2^h. Now d has some period modulo 2^h, say 2^k. Then one can calculate y_0 such that any solution $y \equiv y_0 \bmod 2^k$. Suppose $p = 2^k + 1$ is a Fermat prime. Then $d^{2^k} \equiv 1 \bmod p$ by Fermat's little theorem, and $2^k \equiv -1 \bmod p$. Thus,

$$\begin{aligned} a \cdot 2^x &\equiv cd^{y_0 + m2^k} + e \pmod p, \\ a \cdot 2^x &\equiv cd^{y_0} + e \pmod p, \\ (a \cdot 2^x)^{2k} &\equiv (cd^{y_0} + e)^{2k} \pmod p, \\ a^{2k} &\equiv (cd^{y_0} + e)^{2k} \pmod p. \end{aligned}$$

When there is no solution for $x \geq h$, numerical results suggest that the left and right sides of this final equation are as random as $2k$th powers can be. Thus, with the prime 65537 and our choices of d, the probability seems to be about one out of two thousand that these two sides will be equal.

3. The preprocessing step

We now discuss the important preprocessing step. One can easily calculate by hand the period β of d mod any desired power of b. For instance, when $b = 3$ and $d = 7$, $\beta = \beta(h) = 3 \cdot 3^{h-2}$ is the period of d modulo b^h. Similarly, for 3 and 5 we find $\beta(h) = 2 \cdot 3^{h-1}$, and for 5 and 7 we find $\beta(h) = 4 \cdot 5^{h-2}$.

One now uses [2] or Macsyma to find small prime factors p of $d^\beta - 1$, especially prime factors for which the period $\pi(b, p)$ of b modulo p will be very small. The speed of our algorithm will depend on finding the small p and especially finding small $\pi(b, p)$ with large common factors. In our preprocessing step, therefore, we need to find some small primes p that will give appropriate $\pi(b, p)$.

There always seemed to be an abundance of good candidates. For instance, when $b = 3$ and $d = 7$, with $h = 3$, the primes 19, 37 and 1063 divide $d^\beta - 1$. Since $\pi(b, 1063)$ is quite large, we ignore it. But fortunately, $\pi(b, 19) = \pi(b, 37) = 18$, and so these are fortuitous prime divisors. Roughly half of all the equations $ab^x = cd^y + e$ will fail to have any corresponding x_{37} when viewed mod 37, and of the remaining, only about 1 out of 18 will have the $x_{19} \equiv x_{37} \bmod 18$. Now we might consider $h = 6$. We have several additional divisors, including 109, 811, 1621, 2377, and 3727. When we calculate the $\pi(b, p)$, we notice two fortuitous outcomes: $\pi(b, 1621) = 45$ and $\pi(b, 109) = 27$. The 1621 result is exceptional, since it suggests that roughly 35 out of 36 equations will fail to have any x_{1621}. And those equations for which both x_{1621}

and x_{109} exist have either a solution with $x \geq h = 6$ or else seem to have only roughly one chance in nine of satisfying $x_{1621} \equiv x_{109} \bmod 9$. Consequently, in our preprocessing step, we single out these primes as the ones to use in our algorithm. At this point, one could continue with a higher h, but in fact one can switch the roles of the b and d to locate fortuitous primes dividing powers of b minus one.

These small primes are sufficient to show that almost all equations have no solutions with $x \geq 6$ (and after switching the roles of b and d, $y \geq 5$). When $b = 3$ and $d = 7$, only ten equations remained to be checked, but generally the number of equations left after running the Pascal program was a few dozen. One can actually find the solutions of these equations, choose an h larger than any solution found, and find any two prime divisors of $d^{\beta} - 1$ whose $\pi(b, p)$ have some reasonably large common factor. With so few remaining equations, no cleverness is needed in the preprocessing. Use Macsyma or another infinite-precision arithmetic program to find two such prime divisors and their periods, then apply the algorithm and find an appropriate contradiction for each remaining equation.

4. Conclusions

All equations of the form $ab^x = cd^y + e$ with b and d primes less than or equal to 13, with $a \leq 50$, with $c \leq 50$ and with $|e| \leq 1000$ were tested as described. (Our method does not require b and d to be prime, but the application to the Katai problem will.) As the value of h was increased, the output was checked to make sure that all equations with solutions satisfying $x \geq h$ did indeed pass the tests. This was done to detect programming errors. Indeed, the entire program was written for ease of coding and debugging, certainly not for speed of execution. For a given pair of primes b and d in our range, the program generally took about an hour of CPU time, but a few pairs ranged beyond two hours (depending on the fortuitous nature of the p and $\pi(b, p)$; $d = 11$ seemed to be the worst). While within Pascal's integer range, the programming was done in Pascal on a VAX6310; the few remaining equations were handled using Macsyma on a MicroVax. Every equation in this range was shown to yield a contradiction, proving that no equation of the form $ab^x = cd^y + e$ with our range of parameters has a solution exceeding $x = 18$ (the equation $25 \cdot 2^{18} = 37 \cdot 3^{11} - 839$ gave the largest solution).

When $b = 2$, and one uses only the Fermat primes, one finds that only two equations fail to reach a contradiction in our Fermat prime test: the equation $25 \cdot 2^{18} = 37 \cdot 3^{11} - 839$ noted above and also $2^{15} = 15 \cdot 13^3 - 187$. To use the Fermat method on the first equation, we need to set $h > 18$ but then the period of 3 modulo 2^{19} exceeds 65537, so the Fermat prime method is useless for this equation. The second equation is interesting. The prime 65537 presumably has one chance out of two thousand of failing to prove that this equation has no higher solutions. But this second equation fails to reach a contradiction with the Fermat prime method. The equation is easily handled by going beyond the Fermat primes, that is, explicitly using the $d = 13$ value, but it illustrates the element of "chance" in finding a contradiction for each equation.

We should say a few words about the crucial observation. This algorithm depends on the ability to efficiently find a contradiction. Our crucial observation

says that when no solution with $x \geq h$ exists, then the values x_p for our set of primes are unrelated, hence they usually will not be equivalent. To check whether the values of the x_p are unrelated, we may consider the following results. Consider all equations of the form $ab^x = cd^y + e$ with $b = 3$, $d = 7$, $a \leq 50$, $c \leq 50$, and $|e| \leq 1000$. Disregard all equations where a, b, c, d, and e are not mutually coprime, or which do not have a solution for y_0. Recall that the primes 19 and 37 divide $7^9 - 1$. We calculate the x-values for each equation modulo 19 and 37. The 3237 equations with a solution $x \geq 3$ must have $x_{19} \equiv x_{37} \bmod 18$, so we eliminate these. Of the remaining equations, only 73188 have solutions for both the x_{19} and the x_{37}. For these 73188 equations, one wonders whether the two x values are associated. If one calculates the correlation coefficient, one gets -0.02738. This suggests that there is no (linear) relationship between the values of x_{19} and x_{37}. In fact, only 2935 of the equations have $x_{19} \equiv x_{37} \bmod 18$. The other 70253 equations yield the contradiction $x_{19} \not\equiv x_{37} \bmod 18$ which proves they have no solution with $x \geq 3$.

Acknowledgments

The author thanks Professor R. K. Guy for his careful reading and many helpful suggestions, as well as the referee for many suggestions and for pointing me to the outstanding work of De Weger [3]. The author also thanks Professor O. Marrero for advice concerning the statistical questions, and for running a SAS program with the data.

Bibliography

1. Alan Baker, *Transcendental number theory*, Cambridge Univ. Press, Cambridge, 1975.
2. John Brillhart, D. H. Lehmer, J. L. Selfridge, Bryant Tuckerman, and S. S. Wagstaff, Jr., *Factorizations of* $b^n \pm 1$, Contemp. Math., vol. 22, Amer. Math. Soc., Providence, RI, 1983.
3. B. M. M. De Weger, *Solving exponential Diophantine equations using lattice basis reduction algorithms*, J. Number Theory **26** (1987), 325–367.
4. R. K. Guy, C. B. Lacampagne, and J. L. Selfridge, *Primes at a glance*, Math. Comp. **48** (1987), 183–202.
5. Reese Scott, *On the equation* $p^n - q^m = c$ *and* $|p^n - q^m| = c$, J. Number Theory (to appear).
6. Robert Styer, *A problem of Katai on sums of additive functions*, Acta Sci. Math. (Szeged) **55** (1991), 269–286.

Department of Mathematical Sciences, Villanova University, Villanova, Pennsylvania 19085
E-mail address: styer@ucis.vill.edu