A Note on an Exponential Equation

Rex H. Wu
SUNY, Brooklyn

In [1], Norman Schaumberger provided a positive integer solution to

$$x^{11} = y^4 + z^7 + w^9$$

with $x = 3^{(10!+1)/11}$, $y = 3^{10!/4}$, $z = 3^{10!/7}$, and $w = 3^{10!/9}$. In general,

$$(x_0, x_1, x_2, \ldots, x_n) = \left(n^{((k_0-1)!+1)/k_0}, n^{(k_0-1)!/k_1}, n^{(k_0-1)!/k_2}, \ldots, n^{(k_0-1)!/k_n}\right)$$

is a solution to

$$x_0^{k_0} = x_1^{k_1} + x_2^{k_2} + \ldots + x_n^{k_n}$$

provided k_0 is prime and $k_i \mid (k_0-1)!$ for $i = 1, 2, \ldots, n$. The reason for this is

$$(1) \qquad \left(m^{(q+1)/k_0}\right)^{k_0} = m^{q+1} = m \cdot m^q = \sum_{i=1}^{m} m^q = \sum_{i=1}^{m} \left(m^{q/k_i}\right)^{k_i},$$

since k_0 is a prime, if we choose $q = (k_0 - 1)!$ then from Wilson's Theorem $(q + 1)/k_0$ is an integer, and $k_i \mid q$ for each i.

In this note, we will use this idea to develop solutions to

$$(2) \qquad a_0 x_0^{k_0} = \sum_{i=1}^{n} x_i^{k_i}.$$

We do not require that the k_i be distinct. To avoid trivial cases, we will take $n > 1$.

Theorem 1 *If $a_0 \mid n$ and $gcd(k_0, k_i) = 1$ for $i = 1, 2, \ldots, n$ then (2) has a solution in positive integers.*

Proof: It suffices to show that there is a q such that $k_0 \mid (q+1)$ and $k_i \mid q$ for $i = 1, 2, \ldots, n$. Then we can apply (1).

Let M =lcm$(k_1, k_2, \ldots, k_n)$. Then there exists an integer x such that $q = Mx$ and $k_0 \mid (Mx+1)$. This is so because $\gcd(k_0, k_i) = 1$, which implies $\gcd(k_0, M) = 1$, and $Mx + 1 \equiv 0 \pmod{k_0}$ has a solution if $\gcd(k_0, M) = 1$.

Next, apply (1) and let $m = n/a_0$. Then m is an integer and

$$a_0 \cdot \left[(n/a_0)^{(q+1)/k_0}\right]^{k_0} = a_0 \cdot m^{q+1} = a_0 \cdot m \cdot m^q = n \cdot m^q$$

$$= \sum_{i=1}^{n} m^q = \sum_{i=1}^{n} \left(m^{q/k_i}\right)^{k_i} = \sum_{i=1}^{n} \left[(n/a_0)^{q/k_i}\right]^{k_i}.$$

Thus

$$(x_0, x_1, x_2, \ldots, x_n) = \left((n/a_0)^{(q+1)/k_0}, (n/a_0)^{q/k_1}, (n/a_0)^{q/k_2}, \ldots, (n/a_0)^{q/k_n}\right)$$

is a solution. □

For example, let us find a solution to $x^{11} = y^4 + z^7 + w^9$ using the theorem. Here $a_0 = 1$ and $n = 3$. Since $1 \mid 3$ and gcd(11,4)=gcd(11,7)=gcd(11,9)=1, there exists a solution. We have $m = 3$ and M=lcm$(4, 7, 9) = 252$. Solving $252v + 1 \equiv 0 \pmod{11}$ gives $v \equiv 1 \pmod{11}$. So, taking $q = 252$ would give a solution, specifically $(x, y, z, w) = (3^{23}, 3^{63}, 3^{36}, 3^{28})$.

From the proof to Theorem 1, it is not difficult to see that there is an infinite number of solutions to equation (2) if it satisfies the conditions in Theorem 1. It can be proved in two ways. (I) There is an infinite number of integers satisfying the equation $Mx + 1 \equiv 0 \pmod{k_0}$. (II) Multiply both sides of equation (2) by s^{tQ}, where s and t are positive integers and Q=lcm$(k_0, k_1, k_2, ..., k_n)$. It is also interesting to point out that (II) generates more solutions than (I) in the sense that all solutions generated by (I) form a proper subset of those generated by (II).

While $\gcd(k_0, k_i) = 1$ and $a_0 \mid n$ are sufficient conditions for (2) to have a solution, they are not necessary. There may still be solutions if $\gcd(k_0, k_i) \neq 1$ for some (but not all) i. The next theorem determines some.

Theorem 2 *If $a_0 = t^s$, $n = r^s$, $t \mid r$, and gcd$(k_0, M) \mid (ck_0 - s)$ where M =lcm$(k_1, k_2, \ldots, k_n)$ and c is an integer, then (2) has a solution in positive integers.*

Proof: Since $\gcd(k_0, M) \mid (ck_0 - s)$, the congruence $Mx + s \equiv 0 \pmod{k_0}$ has a solution. Now let $q = Mx$. Then

$$(x_0, x_1, x_2, \ldots, x_n) = \left((r/t)^{(q+s)/k_0}, (r/t)^{q/k_1}, (r/t)^{q/k_2}, \ldots, (r/t)^{q/k_n}\right)$$

is a solution, as can be seen from

$$a_0 \cdot \left[(r/t)^{(q+s)/k_0}\right]^{k_0} = a_0(r/t)^{q+s} = t^s(r/t)^s(r/t)^q = r^s(r/t)^q$$

$$= n(r/t)^q = \sum_{i=1}^{n} \left[(r/t)^{q/k_i}\right]^{k_i}.$$

□

For example, to find a solution to $x_0^{14} = x_1^2 + 2x_2^5 + x_3^6$, we have $n = 4 = 2^2$, M =lcm$(2, 5, 6) = 30$, $\gcd(14, 30) = 2$ and $2 \mid (14 - 2)$, so the equation has a solution. Solve $30v + 2 \equiv 0 \pmod{14}$ to obtain $v \equiv 6$ or $13 \pmod{14}$. If we take $v = 6$, then $q = 180$ and a solution is $(x_0, x_1, x_2, x_3) = (2^{13}, 2^{90}, 2^{36}, 2^{30})$.

There are many difficult questions that can be asked about exponential equations. The two theorems do not provide all solutions to an equation even if their conditions are met. Is there an algorithm that can generate more or even all solutions? Can we determine when (2) does not have any solutions? Obviously, the theorems fail to find solutions for certain equations. For instance, $x^2 = y^3 + z^4$ has a solution, namely, $(x, y, z) = (3, 2, 1)$. A special case of the equation is $x_0^{k_0} = x_1^{k_1} + x_2^{k_2}$ with k_0, k_1 and $k_2 > 2$. Can we conclude that if this equation has a solution then $\gcd(k_0, k_1)$=$\gcd(k_0, k_2) = 1$? (Theorem 2 fails to give a counterexample for this hypothesis.) If the above were true, Fermat's Last Theorem would be a corollary.

Acknowledgement. I wish to thank Susan Hom and Shi-Feng Lu for reviewing this paper.

Reference

1. Norman Schaumberger, Quickie Q795, *Mathematics Magazine* **49** (1992) #4, 266, 273.

Rex Wu received his bachelor's degree in mathematics from New York University. His favorite subjects are algebra and number theory.

Appeared on the *Pi Mu Epsilon Journal* 10(1), pp. 22-25 (1994).