Algorithm Outline for Theorem 1.8 in the draft paper 'On a conjecture concerning the number of solutions to $a^x + b^y = c^z$.'

26 July 2022

For a given prime value of b and some small prime p (or small prime power), we will consider all solutions $(x_1, y_1, x_2, y_2, z_2)$ to $2^{x_1} + b^{y_1} \equiv c \bmod p$ and $2^{x_2} + b^{y_2} \equiv c^{z_2} \bmod p$. Note that the exponents are defined modulo $p - 1$.

When $b \equiv 13 \bmod 24$ and $c \equiv 5 \bmod 24$, we must have $x_1 = 2$. So we have $x_1 = 2$, $2 \mid y_1$, $2 \mid x_2$, $2 \nmid y_2$, $2 \nmid z_2$, and z_2 divides the class number of $\mathbb{Q}(-b)$.

For a given $b \equiv 13 \bmod 24$ we find all $z_2 > 1$ with z_2 odd and dividing the class number. Fix b and z_2. For a given prime p, we consider each $y_1 \bmod p-1$ with y_1 even. Define $c \equiv 2^2 + b^{y_1} \bmod p$; for each value of x_2 even and y_2 odd modulo $p-1$, we see if $2^{x_2} + b^{y_2} \equiv c^{z_2} \bmod p$. If there is a solution, we add (y_1, x_2, y_2) to a list of all possible solutions modulo this prime p.

We now consider another small prime p_2 and look for solutions to $2^{x_1} + b^{y_1} \equiv c \bmod p_2$ and $2^{x_2} + b^{y_2} \equiv c^{z_2} \bmod p_2$ which are consistent with a solution $(y_{1,0}, x_{2,0}, y_{2,0})$ already found modulo p. Specifically, let $m = \gcd(p-1, p_2-1)$. For each solution $(y_{1,0}, x_{2,0}, y_{2,0})$ on the list modulo p, we check $c \equiv 2^2 + b^{y_1} \bmod p_2$ and $2^{x_2} + b^{y_2} \equiv c^{z_2} \bmod p_2$ for values of (y_1, x_2, y_2) for which $y_1 \equiv y_{1,0} \bmod m$, $x_2 \equiv x_{2,0} \bmod m$, and $y_2 \equiv y_{2,0} \bmod m$. For instance, if $p = 5$ and $p_2 = 13$, we only need to check 3^3 tuples (y_1, x_2, y_2) modulo 13 rather than 6^3 possible tuples. If we are fortunate, there are no solutions modulo 13 that are consistent with a solution modulo 5, in which case this choice of b and z_2 cannot have any solutions.

Now we strategically choose a prime p_3. For instance, if $p = 5$, $p_2 = 13$, and $p_3 = 37$, then a solution $(y_1, x_2, y_2) \bmod 37$ will have $y_1 \equiv y_{1,0} \bmod 12$, etc., so we only need to check 3^3 new tuples modulo 37. Similarly, if we next consider $p_4 = 73$ we only need to check 2^3 tuples to find solutions modulo 73 that are consistent with the previous solutions modulo 37.

In this way, we can efficiently check tuples (y_1, x_2, y_2). Often, checking consistency of solutions for only a few primes, we find that a given b, z_2 has no solutions. A few values of b needed multiple primes or prime powers to eliminate.

For $b \equiv 13 \bmod 24$ and $c \equiv 17 \bmod 24$, we must have $x_2 = 2$. The procedure is similar except that we now consider tuples (x_1, y_1, y_2).

For $b \equiv 1 \bmod 24$, we do not have specific values available for x_1 and x_2 but the same essential algorithm can be used for tuples (x_1, y_1, x_2, y_2) although there are now far more cases to test.

In practice, we first used Maple® to get all consistent solutions modulo 5, 7, 9, and 13 for all possible $b \bmod 24 \cdot 5 \cdot 7 \cdot 3 \cdot 13$ and $z_2 \bmod 12$, then used Sage® (in which we could access the Pari® command for class number) to check all relevant primes b and $z_2 > 1$ odd and dividing the class number of $\mathbb{Q}(-b)$ for consistency of solution modulo primes and prime powers. We use primes or prime powers for which $\phi(p)$ has all its prime factors in the set $\{2, 3, 5, 7\}$ (in fact no prime with $7 \mid \phi(p)$ was actually required). The actual primes we used increased somewhat when we found a value of b not eliminated by the then current set of primes, but eventually these were the primes or prime powers used in this order:

37, 73, 109, 163, 243, 81, 181, 271, 19, 27, 61, 31, 241, 97, 193, 257, 17, 41, 25, 101, 125, 151, 11, 211, 71, 29, 43, 49, 127.

In fact, no value of b required any of the values from 25 onwards; presumably with more care even fewer values would be required.

Since we used these primes in our program, we need to verify that these primes do not lead to solutions. For primes $b \equiv 13 \bmod 24$ or $b \equiv 1 \bmod 24$ with $b \leq 271$, only 61, 109, 157, 181, 229,and 241 have an odd factor in the class number. The cases $b = 61$, 109, 181, 229, and 241 are eliminated by consideration modulo 5. The case $b = 157$ is eliminated by consideration modulo 13 and 5.