Lowering the Bound for Connected Markoff Graphs Modulo a Prime

Nico Tripeny

May 25, 2022

Abstract

The Markoff equation $x^2+y^2+z^2-3xyz=0$ has a graph associated to its solutions which is known to be connected over the positive integers. One natural question is whether or not the graph is still connected when we take the solutions to the equations modulo a prime. This was recently shown to be true for large enough primes p using methods from analytic number theory and algebraic geometry [1, 2]. Here, we attempt to refine the methods in order to lower the upper bound p for which the graph is guaranteed to be connected.

1 Background Information

The equation $x^2+y^2+z^2-3xyz=0$ is known as the Markoff equation, with solutions (a,b,c) known as Markoff triples. In order to better understand the properties of these triples, the solutions to the equation can be studied modulo a prime number. For this we look at Markoff triple mod p, any integer triple $(x,y,z)\in\mathbb{F}_p$ satisfying

$$x^2+y^2+z^2-3xyz\equiv 0 \mod p.$$

We also call a number a Markoff number mod p if it appears in some Markoff triple mod p. Since we will be looking at reductions modulo p for large primes, we can instead look at the equation $x^2+y^2+z^2-xyz\equiv 0 \mod p$ as there is a simple transformation between solutions of the two.

One question to ask is whether or not reducing gives new solutions, or if all solutions are reductions of Markoff triples. In order to study this, we can look at the rotations

$$\mathrm{rot}_{x_1}(x_1,x_2,x_3)=(x_1,x_3,x_1x_3-x_2)$$

with rot_{x_2} and rot_{x_3} defined similarly. One can see that rotations send Markoff triples to other Markoff triples. We can describe this rotation using a matrix. Namely,

$$\mathrm{rot}_{x_1}\begin{pmatrix}x_2\\x_3\end{pmatrix}=\begin{pmatrix}0&1\\-1&x_1\end{pmatrix}\begin{pmatrix}x_2\\x_3\end{pmatrix}.$$

We can view this matrix as an element of $\mathrm{SL}_2(\mathbb{F}_p)$ and can then ask the order of each of these elements. We then define the order of x to be the order of this matrix. We can then define the order of a triple (x_1,x_2,x_3) to be the maximal order of each of the elements.

We can now define and study some basic properties of the Markoff graph mod p, $\hat{G}_p$. This is the graph having vertices of Markoff triples mod p and edges between vertices if a rotation takes one vertex to the other. It can be shown that all Markoff triples with positive elements are generated by rotations on $(1,1,1)$ [4]. So, if one shows the graph $\hat{G}_p$ is connected, then all Markoff triples mod p are reductions of regular Markoff triples.

With this goal in mind, we state a few previously known results. Namely, Bougain et al. showed that all triples of maximal order are connected. This connected component is called the cage [1]. The rest of the paper then attempts to connect as much as possible to the cage, and we call this connected component $C(P)$. It can be shown that if a triple has order greater than $p^{\frac{1}{2}+\delta}$ then it is connected to the cage. It was also shown that of the triples with order $d < p^{\frac{1}{2}+\delta}$, only at most $20d^{\frac{1}{3}}d_0^{\frac{1}{3}}$ can be not connected to triples with order greater than d_0.

These results are then enhanced by a result of Will Chen. He showed that every connected component of the Markoff graph mod p is divisible by p [2]. This gives us reason to lower the size of the component not connected to the cage.

2 Bound for size of disconnected components

As mentioned, there is a small $\delta > 0$ such that if a triple has order greater then $p^{\frac{1}{2}+\delta}$ it is part of the connected component with the cage. So, a triple must have smaller order to not be connected to the cage. One can show that a triple must have an order dividing $p+1$ or $p-1$, so we need only look at triples with order less than $p^{\frac{1}{2}+\delta}$ that divide one of these two numbers [1]. In a note by Sarnak detailing the proof of Theorem 1 of Bourgain et al., it is shown that an upper bound

$$|\hat{G}_p \setminus C(p)| \leq 20^6 \cdot 2 \cdot C_\varepsilon^8 p^{16\varepsilon}$$

may be established.
It is introduced that y_p is the least y such that

$$t^{\frac{1}{3}} \sum_{\substack{d \leq t \\ d|(p^2-1)}} 20 \cdot d^{\frac{1}{3}} < t \tag{1}$$

for $t \geq y$. This formula comes from summing over the possible order of a triple not connected to the cage. The $20d^{\frac{1}{3}}t^{\frac{1}{3}}$ is because only that many can be not connected to a triple of order larger than t. The idea is then to notice that triples with order greater than t can then continuously be moved to triples of larger and larger order because of the above inequality. They will then eventually reach the cage. So, this sum gives us a way to bound our disconnected component.
Sarnak bounds the left side of (1) by replacing d with t and getting

$$t^{\frac{1}{3}} \sum_{\substack{d \leq t \\ d|(p^2-1)}} 20 \cdot d^{\frac{1}{3}} \leq 20 \cdot t^{\frac{2}{3}} \cdot \tau(p^2-1) \tag{2}$$

where $\tau(n)$ is the number of divisors of n.
He then uses the fact that for all ε there is a C_ε such that

$$\tau(n) \leq C_\varepsilon n^\varepsilon.$$

We note that this may be improved to

$$\tau(n) \leq n^{\frac{1}{log(log(n))}}$$

By a slight manipulation of a result found on page 262 of [5]. Using this to bound equation (2), we arrive at

$$t^{\frac{1}{3}} \sum_{\substack{d \leq t \\ d|(p^2-1)}} 20 \cdot d^{\frac{1}{3}} \leq 20 \cdot t^{\frac{2}{3}} \cdot p^{\frac{2}{log(log(p^2))}}.$$

However, since d is the order of a triple, it must divide $p-1$ or $p+1$. Then, instead of summing over $d|(p^2-1)$, we may sum over $d|(p+1)$ *or* $(p-1)$, denoting this as $d|(p\pm 1)$. This improves our bound to

$$t^{\frac{1}{3}} \sum_{\substack{d \leq t \\ d|(p\pm 1)}} 20 \cdot d^{\frac{1}{3}} \leq 20 \cdot t^{\frac{2}{3}} \cdot 2 \cdot p^{\frac{1}{log(log(p))}} \tag{3}$$

since we replace $\tau(p^2-1)$ in (2) with $\tau(p+1)+\tau(p-1)$.
Now putting y_p into (3), we get

$$y_p \leq t^{\frac{1}{3}} \sum_{\substack{d \leq y_p \\ d|(p\pm 1)}} 20 \cdot d^{\frac{1}{3}} \leq 20 \cdot y_p^{\frac{2}{3}} \cdot 2 \cdot p^{\frac{1}{log(log(p))}}.$$

Solving for y_p gives

$$y_p < 40^3 \cdot p^{\frac{3}{log(log(p))}}. \tag{4}$$

Now the number of possible elements with order at most y_p is given by

$$\sum_{\substack{d \leq y_p \\ d|(p\pm 1)}} d \leq (\tau(p-1)+\tau(p+1)) \cdot y_p.$$

Since we are creating Markoff triples from these elements, We see we may pair any two elements with order at most y_p. Once we fix two elements of $x^2+y^2+z^2-3xyz=0$, we simply get a quadratic over a field, so there are at most 2 ways to choose the third element. Using our bound for $\tau(p-1)$ and $\tau(p+1)$, we get which gives the number of triples of order at most y_p as

$$2(y_p \cdot 2 \cdot p^{\frac{1}{log(log(p))}})^2.$$

Since this is an upper bound for how many triples can be disconnected from the cage, we may combine this with (4) as an estimate for y_p to see

$$|\hat{G}_p \setminus C(p)| \leq 2(y_p \cdot 2 \cdot p^{\frac{1}{log(log(p))}})^2. \leq 8 \cdot 40^6 \cdot p^{\frac{8}{log(logp)}}.$$

From the result of Will Chen, we now have a way to bound the primes p for which $\hat{G}_p$ can have any disconnected components. If $8 \cdot 40^6 \cdot p^{\frac{8}{log(logp)}} < p$ then we must have the graph $\hat{G}_p$ is connected as we desired.

3 Alternate Formula from the above inequality

From the previous section, we know we want

$$20 \cdot y_p^{\frac{1}{3}} \cdot \sum_{\substack{d \leq y_p \\ d|(p\pm 1)}} d^{\frac{1}{3}} \leq y_p$$

and that approximately this will hold if

$$20 \cdot y_p^{\frac{1}{3}} \cdot \sum_{\substack{d \leq y_p \\ d|n}} d^{\frac{1}{3}} \leq \frac{y_p}{2}$$

for both $n = p-1$ and $n = p+1$, so we will look at these cases. One can also show that

$$\sigma_{\frac{1}{3}}(n) = \sum_{d|n} d^{\frac{1}{3}} = \prod_{p_j|n} \frac{p_j^{(e_j+1)\frac{1}{3}} - 1}{p_j^{\frac{1}{3}} - 1}$$

where p_j is a prime and e_j is the largest power such that $p_j^{e_j}$ divides n. So, we see

$$\sum_{\substack{d \leq y_p \\ d|n}} d^{\frac{1}{3}} = \prod_{p_j|n} \frac{p_j^{(e_j+1)\frac{1}{3}} - 1}{p_j^{\frac{1}{3}} - 1} - \sum_{\substack{d > y_p \\ d|n}} d^{\frac{1}{3}}$$

and therefore may show

$$\prod_{p_j|n} \frac{p_j^{(e_j+1)\frac{1}{3}} - 1}{p_j^{\frac{1}{3}} - 1} - \sum_{\substack{d > y_p \\ d|n}} d^{\frac{1}{3}} \leq \frac{y_p^{\frac{2}{3}}}{40}.$$

From $y_p < 40^3 \cdot p^{\frac{3}{\overline{log(log(p))}}}$, we see y_p is less then $n^{\frac{1}{2}}$ for values of p significantly smaller then when we can assume $8 \cdot 40^6 \cdot p^{\frac{8}{\overline{log(logp)}}} < p$. So, to try to lower the bound we can assume that $y_p < n^{\frac{1}{2}}$ then we see at least half of the divisors of n are in

$$\sum_{\substack{d > y_p \\ d|n}} d^{\frac{1}{3}}$$

so we can see

$$\sum_{\substack{d > y_p \\ d|n}} d^{\frac{1}{3}} \leq \frac{\tau(n)}{2} n^{\frac{1}{6}}.$$

Now if we let $t = \sigma_{\frac{1}{3}}(n)$ we want to show

$$t - \sum_{\substack{d>y_p \\ d|n}} d^{\frac{1}{3}} \leq t - \frac{\tau(n)}{2} n^{\frac{1}{6}} \leq \frac{y_p^{\frac{2}{3}}}{40}.$$

Rearranging, we see

$$t \leq \frac{y_p^{\frac{2}{3}}}{40} + \frac{\tau(n)}{2} n^{\frac{1}{6}}.$$

Finally, if we cube both sides we get

$$t^3 \leq \frac{y_p^2}{40^3} + \frac{(\tau(n))^3}{8} n^{\frac{1}{2}} \leq (\frac{y_p^{\frac{2}{3}}}{40} + \frac{\tau(n)}{2} n^{\frac{1}{6}})^3.$$

4 Comaximal divisors

In the sections above, we were assuming that for all d that could be orders of triples, there are exactly d numbers in $\mathbb{F}_p$ with this order. In reality, however, there are d elements that divide this order. So, if we are summing over both d and d' where $d'|d$, then we are over counting by the sum added from d'.

As we are summing over all divisors of $p \pm 1$ less than or equal to t, we are over counting in this way. We can then instead sum over the comaximal divisors of $p \pm 1$ less than or equal to t, meaning the set of numbers that divide no larger divisor of $p \pm 1$. So, we now want to know the sum

$$\sum_{\substack{d \leq t \\ d|(p\pm 1) \\ d \text{ comaximal}}} 20 \cdot d^{\frac{2}{3}}.$$

Now let us look at finding an upper bound for the amount of comaximal divisors. Instead of the case $d|(p \pm 1)$, we will look at $d|n$ for a more generic n. We will look at the division poset for the number n, meaning the poset where $a \leq b$ if $a|b$ for all numbers a and b dividing n. An antichain in a poset is a set of elements $\{a_i\}$ such that $a_i \leq a_j$ implies $i = j$.

We see that for any upper bound on the elements, the comaximal elements form an antichain in the division poset. So, we may find the largest antichain in that poset. This can be given by all numbers that divide n with half as many prime divisors as n if the number of prime divisors is even, or this value rounded down if the number of prime divisors is odd.

Now, a number n can be viewed as a multiset of primes based on its prime decomposition, so this is the same as asking for the number of sub-multisets of a given multiset with half as many elements, counting multiplicity.

Let $\mathscr{M}$ be a multiset $\{p_1^{a_1}, p_2^{a_2} \cdots, p_k^{a_k}\}$, meaning that the element p_i has multiplicity a_i, I be the base set of $\mathscr{M}$, and $\mathscr{P}(I)$ be the powerset of I. Then the general formula for finding sub-multisets

of a given cardinality m is

$$\sum_{L \in \mathscr{P}(I)} (-1)^{|L|} \binom{m+k-1-|L|-\sum_{i \in L} a_i}{k-1}[3].$$

So putting in half the number of prime divisors of n for m gives the desired maximal antichain. So, finding an upper bound on this value will give an improvement over $p^{\frac{1}{log(log(p))}}$.

The bound could be improved even better by showing that a different antichain can be used as an upper bound for the number of comaximal elements, or finding a precise way of counting these specifically.

5 Conclusion and future research

We have been able to lower the bound for the prime p, but it is still well outside of computational range. Future research as stated could look at the antichains and comaximal divisors. Alternatively, we have only looked at the first layer of orbits when studying connectivity. If we instead look at the orbit of an element and orbits of the elements in that orbit, we may be able to get a better bound. This may then make it possible to search through all remaining primes to show the graph indeed is connected for all primes.

References

[1] Jean Bourgain, Alexander Gamburd, and Peter Sarnak. Markoff Surfaces and Strong Approximation: 1. 2021.

[2] William Chen. Nonabelian Level Structures, Nielsen Equivalence, and Markoff Triples, 2021.

[3] Sebastiano Ferraris, Alex Mendelson, Gerardo Ballesio, and Tom Vercauteren. Counting Sub-Multisets of Fixed Cardinality, 2015.

[4] Elena Fuchs, Kristen Lauter, Matthew Litman, and Austin Tran. A Cryptographic Hash Function from Markoff Triples. *Mathematical Cryptology*, 2021.

[5] G.H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers*. Oxford University Press, 4th edition, 1938.