

Safal Das Biswas
B. Math 3rd year Indian statistical Institute
Number Theory Diophantine equation

1. Prove or Disprove the equation $9X^2 - 10XY + 9Y^2 = Z \uparrow^{2020}$ has infinitely many integer solution X, Y, Z such that $\gcd(X, Y, Z) = 1$, where,

$$Z \uparrow^2 = Z^Z, Z \uparrow^3 = Z^{Z^Z}, Z \uparrow^4 = Z^{Z^{Z^Z}}, \text{ defined analogously for } Z \uparrow^{2020}$$

Solution: We will prove that the equation has infinitely many integer solution.

We will first show that $9X^2 - 10XY + 9Y^2 = Z^Z$ has infinitely many integer solution X, Y, Z such that $\gcd(X, Y, Z) = 1$

The equation is equivalent as $2A^2 + 7B^2 = Z^Z$ where $A = X + Y$ and $B = X - Y$

Claim 1: $(2u^2 + 7v^2)^{2k+1} = 2m^2 + 7n^2$ for some positive integer m, n , and k be any natural number.

$$\begin{aligned} \text{Proof: } (\sqrt{2}u + \sqrt{-7}v)^{2k+1} &= \sum_{m=0}^{2k+1} \binom{2k+1}{m} (\sqrt{2}u)^m (\sqrt{-7}v)^{2k+1-m} \\ &= \sum_{m \text{ odd}} \binom{2k+1}{m} (\sqrt{2}u)^m (\sqrt{-7}v)^{2k+1-m} + \sum_{m \text{ even}} \binom{2k+1}{m} (\sqrt{2}u)^m (\sqrt{-7}v)^{2k+1-m} \\ &= \sqrt{2} \sum_{m \text{ odd}} \binom{2k+1}{m} 2^{\frac{m-1}{2}} (-7)^{\frac{2k+1-m}{2}} u^m v^{2k+1-m} + \\ &\quad \sqrt{-7} \sum_{m \text{ even}} \binom{2k+1}{m} 2^{\frac{m}{2}} (-7)^{\frac{2k+1-m-1}{2}} u^m v^{2k+1-m} \end{aligned}$$

$$\text{Pick } m = \sum_{m \text{ odd}} \binom{2k+1}{m} 2^{\frac{m-1}{2}} (-7)^{\frac{2k+1-m}{2}} u^m v^{2k+1-m} \text{ and}$$

$$n = \sum_{m \text{ even}} \binom{2k+1}{m} 2^{\frac{m}{2}} (-7)^{\frac{2k+1-m-1}{2}} u^m v^{2k+1-m}$$

$$\text{Thus, } (\sqrt{2}u + \sqrt{-7}v)^{2k+1} = \sqrt{2}m + \sqrt{-7}n \text{ and } (\sqrt{2}u - \sqrt{-7}v)^{2k+1} = \sqrt{2}m - \sqrt{-7}n$$

$$\text{Thus, } (2u^2 + 7v^2)^{2k+1} = (\sqrt{2}m + \sqrt{-7}n)(\sqrt{2}m - \sqrt{-7}n) = 2m^2 + 7n^2 \quad \blacksquare$$

$$\text{Take } v = 1, \text{ and let } A_{2k+1} = \sum_{m \text{ odd}} \binom{2k+1}{m} 2^{\frac{m-1}{2}} (-7)^{\frac{2k+1-m}{2}} u^m \text{ and set}$$

$$B_{2k+1} = \sum_{m \text{ even}} \binom{2k+1}{m} 2^{\frac{m}{2}} (-7)^{\frac{2k+1-m-1}{2}} u^m$$

Claim 2: For every prime $p|2u^2 + 7$, we have $\frac{A_{2k+1}}{u} \equiv B_{2k+1} \pmod{p}$

$$\text{Proof: } \frac{A_{2k+1}}{u} = \left(\binom{2k+1}{1} (-7)^k + \binom{2k+1}{3} 2(-7)^{k-1}u^2 + \dots + \binom{2k+1}{2k+1} (2)^k u^{2k} \right)$$

$$\frac{A_{2k+1}}{u} = \left(\binom{2k+1}{2k} (-7)^k + \binom{2k+1}{2k-2} 2(-7)^{k-1}u^2 + \dots + \binom{2k+1}{0} (2)^k u^{2k} \right)$$

$$B_{2k+1} = \left(\binom{2k+1}{2k} 2^k u^{2k} + \binom{2k+1}{2k-2} 2^{k-1}(-7)u^{2k-2} + \dots + \binom{2k+1}{0} (-7)^k \right)$$

$$2u^2 \equiv -7 \pmod{p} \Rightarrow (-7)^k \equiv 2^k u^{2k} \pmod{p}, 2(-7)^{k-1}u^2 \equiv 2^{k-1}(-7)u^{2k-2} \pmod{p}$$

and so on for each binomial coefficient thus $\frac{A_{2k+1}}{u} \equiv B_{2k+1} \pmod{p}$ ■

Now we are near to end, choose 7 not divides u, Clearly A_{2k+1} and B_{2k+1} is odd with

u odd since $2k+1 | \binom{2k+1}{i}$ for $1 \leq i \leq k-1$,

$$2u^2 + 7 | \binom{2u^2+7}{i}, \text{ and } 2u^2 + 7 \nmid A_{2u^2+7} \text{ thus by claim 1 } 2u^2 + 7 \nmid B_{2u^2+7}$$

thus $2A_{2u^2+7}^2 + 7B_{2u^2+7}^2 = (2u^2 + 7)^{2u^2+7}$, as by Claim 2 for any prime $p|2u^2 + 7$

$p \nmid A_{2u^2+7}$ thus $\gcd(A_{2u^2+7}, B_{2u^2+7}, 2u^2 + 7) = 1$,

Observe that one can replace $2u^2 + 7$ with $(2u^2 + 7)k$ in exponent where k odd

and we have $2A_{(2u^2+7)k}^2 + 7B_{(2u^2+7)k}^2 = (2u^2 + 7)^{(2u^2+7)k}$

with $\gcd(A_{(2u^2+7)k}, B_{(2u^2+7)k}, 2u^2 + 7) = 1$, Since $(2u^2 + 7) \uparrow^n = (2u^2 + 7)k$

$$\text{Now } X_{(2u^2+7) \uparrow^n} = \frac{A_{(2u^2+7) \uparrow^n} + B_{(2u^2+7) \uparrow^n}}{2}, Y_{(2u^2+7) \uparrow^n} = \frac{A_{(2u^2+7) \uparrow^n} - B_{(2u^2+7) \uparrow^n}}{2}$$

As $A_{(2u^2+7) \uparrow^n}$ and $B_{(2u^2+7) \uparrow^n}$ odd both $X_{(2u^2+7) \uparrow^n}$ and $Y_{(2u^2+7) \uparrow^n}$ are integers

$$\gcd\left(\frac{A_{(2u^2+7) \uparrow^n} + B_{(2u^2+7) \uparrow^n}}{2}, \frac{A_{(2u^2+7) \uparrow^n} - B_{(2u^2+7) \uparrow^n}}{2}\right)$$

$$= \gcd\left(A_{(2u^2+7) \uparrow^n}, \frac{A_{(2u^2+7) \uparrow^n} - B_{(2u^2+7) \uparrow^n}}{2}\right) = A \text{ (say), clearly } A \text{ must be odd, thus}$$

let p be a prime such that $p|A_{(2u^2+7) \uparrow^n}$ if $p|A$ then $p| \frac{A_{(2u^2+7) \uparrow^n} - B_{(2u^2+7) \uparrow^n}}{2}$ then $p|B_{(2u^2+7) \uparrow^n}$

$$\begin{aligned} & \text{but } \gcd(A_{(2u^2+7)\uparrow^n}, B_{(2u^2+7)\uparrow^n}) \\ & = 1 \text{ so contradiction thus } \gcd\left(\frac{A_{(2u^2+7)\uparrow^n} + B_{(2u^2+7)\uparrow^n}}{2}, \frac{A_{(2u^2+7)\uparrow^n} - B_{(2u^2+7)\uparrow^n}}{2}\right) \\ & = 1 \end{aligned}$$

Hence $\gcd(X_{(2u^2+7)\uparrow^n}, Y_{(2u^2+7)\uparrow^n}, (2u^2 + 7) \uparrow^n) = 1$ completing the proof.

Contact of Author: Name: Safal Das Biswas

Email: safaldasbiswas@gmail.com
