TSTST 2020/4

Evan Chen

Twitch Solves ISL

Episode 44

Problem

Find all pairs of positive integers (a, b) satisfying the following conditions:

(i) a divides $b^4 + 1$,

(ii) b divides $a^4 + 1$,

(iii) $\lfloor \sqrt{a} \rfloor = \lfloor \sqrt{b} \rfloor$.

Video

https://youtu.be/FozF63KHw6E

Solution

The only solutions are $(1,1)$, $(1,2)$, and $(2,1)$, which clearly work. Now we show there are no others.

Obviously, $\gcd(a,b)=1$, so the problem conditions imply

$$ab \mid (a-b)^4+1$$

since each of a and b divide the right-hand side. We define

$$k \overset{\text{def}}{=} \frac{(b-a)^4+1}{ab}.$$

Claim (Size estimate)**.** We must have $k \le 16$.

Proof. Let $n = \lfloor \sqrt{a} \rfloor = \lfloor \sqrt{b} \rfloor$, so that $a, b \in [n^2, n^2+2n]$. We have that

$$\begin{gathered} ab \ge n^2(n^2+1) \ge n^4+1 \\ (b-a)^4+1 \le (2n)^4+1 = 16n^4+1 \end{gathered}$$

which shows $k \le 16$. □

Claim (Orders argument)**.** In fact, $k=1$.

Proof. First of all, note that k cannot be even: if it was, then a, b have opposite parity, but then $4 \mid (b-a)^4+1$, contradiction.

Thus k is odd. However, every odd prime divisor of $(b-a)^4+1$ is congruent to 1 (mod 8) and is thus at least 17, so $k=1$ or $k \ge 17$. It follows that $k=1$. □

At this point, we have reduced to solving

$$ab = (b-a)^4+1$$

and we need to prove the claimed solutions are the only ones. Write $b=a+d$, and assume WLOG that $d \ge 0$: then we have $a(a+d)=d^4+1$, or

$$a^2 - da - (d^4+1) = 0.$$

The discriminant $d^2+4(d^4+1) = 4d^4+d^2+4$ must be a perfect square.

- The cases $d=0$ and $d=1$ lead to pairs $(1,1)$ and $(1,2)$.
- If $d \ge 2$, then we can sandwich

  $$(2d^2)^2 < 4d^4+d^2+4 < 4d^4+4d^2+1 = (2d^2+1)^2,$$

  so the discriminant is not a square.

The solution is complete.

Remark (Author remarks on origin)**.** This comes from the problem of the existence of a pair of elliptic curves over $\mathbb{F}_a$, $\mathbb{F}_b$ respectively, such that the number of points on one is the field size of the other. The bound $n^2 \le a, b < (n+1)^2$ is the Hasse bound. The divisibility conditions correspond to asserting that the embedding degree of each curve is 8, so that they are *pairing friendly*. In this way, the problem is essentially the key result of `https://arxiv.org/pdf/1803.02067.pdf`, shown in Proposition 3.