USEMO 2020/6

Evan Chen

Twitch Solves ISL

Episode 35

Problem

Prove that for every odd integer $n > 1$, there exist integers $a, b > 0$ such that, if we let $Q(x) = (x + a)^2 + b$, then the following conditions hold:

- we have $\gcd(a, n) = \gcd(b, n) = 1$;
- the number $Q(0)$ is divisible by n; and
- the numbers $Q(1)$, $Q(2)$, $Q(3)$, ... each have a prime factor not dividing n.

Video

https://youtu.be/uj93tNL8f7M

Solution

Let $p_1 < p_2 < \cdots < p_m$ denote the odd primes dividing n and call these primes *small*. The construction is based on the following idea:

Claim. For each $i = 1, \dots, m$ we can choose a prime $q_i \equiv 1 \pmod 4$ such that

$$\left(\frac{p_j}{q_i}\right) = \begin{cases} -1 & \text{if } j = i \\ +1 & \text{otherwise.} \end{cases}$$

Proof. Fix i. By quadratic reciprocity, it suffices that $q_i \equiv 1 \pmod 4$ and that q_i is a certain nonzero quadratic residue (or not) modulo p_j for $j \neq i$.

By Chinese remainder theorem, this is a single modular condition, so Dirichlet theorem implies such primes exist. □

We commit now to the choice

$$b = kq_1q_2 \dots q_m$$

where $k \geq 1$ is an integer (its value does not affect the following claim).

Claim (Main argument)**.** For this b, there are only finitely many integers X satisfying the equation

$$X^2 + b = p_1^{e_1} \dots p_m^{e_m} \qquad (\spadesuit)$$

where e_i are some nonnegative integers (i.e. $X^2 + b$ has only small prime factors).

Proof. In ($\spadesuit$) the RHS is a quadratic residue modulo b. For any $i > 0$, modulo q_i we find

$$+1 = \prod_j \left(\frac{p_i^{e_i}}{q_i}\right) = (-1)^{e_i}$$

so e_i must be even. This holds for every i though! In other words all e_i are even.

Hence ($\spadesuit$) gives solutions to $X^2 + b = Y^2$, which obviously has only finitely many solutions. □

We now commit to choosing any $k \geq 1$ such that

$$k \equiv -\frac{1}{q_1q_2 \dots q_m} \pmod n$$

which in particular means $\gcd(k, n) = 1$. Now as long as $a \equiv 1 \pmod n$, we have $Q(0) \equiv 0 \pmod n$, as needed. All that remains is to take a satisfying the second claim larger than any of the finitely many bad integers in the fist claim.

Remark (Motivational comments from Nikolai Beluhov)**.** The solution I ended up with is not particularly long or complicated, but it was absurdly difficult to find. The main issue I think is that there is nothing in the problem to latch onto; no obvious place from which you can start unspooling the yarn. So what I did was throw an awful lot of different strategies at it until one stuck.

Eventually, what led me to the solution was something like this. I decided to focus on the simplest nontrivial case, when n contains just two primes. I spent some time thinking about this, and then at some point I remembered that in similar Diophantine equations I've seen before, like $2^x + 3^y = z^2$ or $3^x + 4^y = 5^z$, the main trick is first of all to prove that the exponents are even. After that, we can rearrange and factor a difference of squares. This idea turned out to be fairly straightforward to implement, and this is how I found the solution above.

Remark (The problem is OK with n even)**.** The problem works equally well for n even, but the modifications are both straightforward and annoying, so we imposed n odd to reduce the time taken in solving this problem under exam conditions.

On the other hand, for odd n, one finds that a simplified approach is possible where one proves the main argument by choosing $b \equiv 2 \pmod 4$ and then using the quadratic reciprocity argument to force the right-hand side of (♠) to be $1 \pmod 4$. In this case, there are no integers X at all satisfying (♠), and the "sufficiently large" leverage provided by the choice of a is not needed.

Remark (On the choice of conditions)**.** The equation (♠), and the goal to show it has finitely many solutions (or no solutions), is the heart of the problem. But the other conditions have been carefully chosen to prevent two "trivial" constructions to this.

If the condition that $\gcd(a, n) = \gcd(b, n) = 1$ or $n \mid Q(0)$ is dropped, the problem becomes much easier because one can simply ensure that $\nu_p(Q(x))$ is bounded for all $p \mid n$, by taking $b = n$ (or $b = \operatorname{rad} n$, etc.). However, these two conditions jointly together ensure that $\nu_p(Q(x))$ may be unbounded, by a Hensel-type argument.

If $b < 0$ is permitted, an easier approach to make sure that $Q(x)$ factors as the product of two polynomials by requiring b to be the negative of a perfect square. Several easier approaches become possible in this situation. For example, one can try to use Kobayashi's theorem to generate the value of a after ensuring the first two conditions are true.

Remark (Author remarks on generalization)**.** In general, it seems like *any* b satisfying $\gcd(b, n) = 1$ should still have finitely many solutions to (♠). The author comments that this would be a statement of Kobayashi's theorem in the ring of integers of the quadratic field $\mathbb{Q}(\sqrt{-b})$, but the organizers of the competition were not able to locate such a statement in the literature.