AceBear Security Contest 2019

Challenge: *cotan*

Hi everyone,

Welcome to the *cotan* challenge, I hope you still remember this formula:

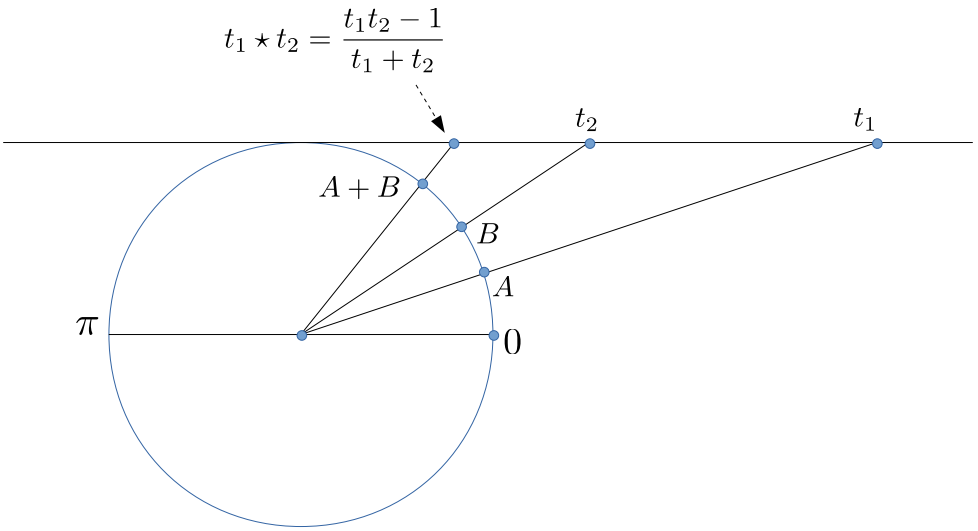
$$cot(A+B) = \frac{cot(A)cot(B)-1}{cot(A)+cot(B)} \tag{1}$$

Let's define a new operation, $\star$, for which $t_1 \star t_2 = \frac{t_1 t_2 - 1}{t_1 + t_2}$, then we can rewrite (1) as

$$cot(A+B) = cot(A) \star cot(B) \tag{2}$$

Let $+_\pi$ denote addition modulo π, then this subset of $\mathbb{R}$: $[0, \pi)$ (including 0 but not π) under $+_\pi$ is clearly a group (in fact, it is the quotient group $\frac{\mathbb{R}}{2\pi\mathbb{R}}$).

Now, it's time to introduce another group. Let f be a mapping which maps $x \in [0, \pi)$ to $cot(x) \in \mathbb{R} \cup \{\infty\}$, then f carries the group structure of $[0, \pi)$ under $+_\pi$ to $R \cup \{\infty\}$ under $\star$ (see the figure below).



And here's the challenge for you. We will be working on F_p instead of $\mathbb{R}$. I give you $\underbrace{2 \star 2 \star 2 \star ...2}_{\text{k times}}$ and you need to find k, that's all. Good luck!