

Comentarios a *Problems when dealing with big integers*

challenge-response

En aquest comentari (tot el primer paràgraf) et refereix

aquello que se co

... dado C y B mal

... En ese caso el incentivo será doble, la gente

... alizados) y paralelamente a eso estará incentivados ha trabajar

Assumpció 1: L'execució de la transició més costosa de

... sabotaje podría saturar la plataforma si comienza a enviar

... las envía todas de forma directa solo se le podrá penalizar un

... todo el sistema por el exceso de verificaciones, y quizás después,

... excede sus bienes y puede saturar el sistema impunemente. Una

... suceder que tampoco tengo claro si ya tenéis algún mecanismo

... uede ser retener una parte de su GAS en pretexto de no poder

... ión, que posteriormente se devolverá si no hay maldad en sus

... demandas de verificaciones. Fíjate que esto puede también puede constituir un incentivo triple a no

... *jugarse-la* con aproximaciones numéricas.

No entenc molt bé aquesta part, que vol dir? Qui se la jugaria

Comentarios de la subsección *Modular multiplication & addition*

- Como estamos en \mathbb{Z}_p muchos de los cálculos ejecutados son equivalentes a otros, quizás (no lo sé)

puede s

operaci

positivo

incluso

que gue

Hi ha algo que et porti a pensar que hi hauràn càlculs que es repeteixin bastant (degut a la

- Esto es solo un pequeño juego matemático que se me ocurrió para números pequeños. Imaginemos que estamos en \mathbb{Z}_p , supongamos \mathbb{Z}_7 sin pérdida de generalidad y queremos calcular $5 \cdot 6$ pero somos incapaces de efectuar el calculo o bien de poder pensar en un número más grande que 7. **Tenemos que** $5 \cdot 6 \equiv 5 \cdot -1 \equiv -5 \equiv 7$ y no nos hemos pasado de siete.

Un algoritmo de multiplicación interesante puede ser el **Algoritmo de Karatsuba**, a diferencia del clasico que tiene complejidad $\mathcal{O}(n^2)$ este tiene $\mathcal{O}(3n^{\log_2 3})$ aproximadamente 1.584962500... osea que es como $\mathcal{O}(3n^{\log_2 3})$ algorithm

Alguna idea de

El gran problema que tenim amb els algoritmes de