Thank you!

Any questions*?

*If not, I have a question for you…

Constant-time Gauss’ algorithm?

Finite field world

Q: Given $\mathbb{F}_q$ find generator ζ for $\mathbb{F}_q^*$

Curve world

Given curve E over $\mathbb{F}_{p'}$
find full torsion point P