**Constant-time Gauss' algorithm?**

## *Finite field world*

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

## *Curve world*

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

**Constant-time Gauss' algorithm?**

# Finite field world

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

**A:**

**GAUSS' ALGORITHM**

1. Take random $\zeta \in \mathbb{F}_{q'}$ compute $t = \mathsf{Order}(\zeta)$
2. If $t = q - 1$, **stop**,
3. **else** take random $\beta \in \mathbb{F}_q^*$ and compute $s = \mathsf{Order}(\beta)$
   a. if $s = q - 1$, **stop**
   b. **else** find coprime $d \mid t$ and $e \mid s$ with $d \cdot e = \mathsf{lcm}(t, s)$
   c. set $\zeta \leftarrow \zeta^{t/d} \cdot \beta^{s/e}$ and $t \leftarrow d \cdot e$ and **repeat** from 2.

# Curve world

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

Take $P$ and $Q$,
Compute their torsion.
If $P$ not full torsion,
take right multiple $Q$
set $P \leftarrow P + Q$ to fill
missing torsion in $P$
repeat until full torsion