Constant-time Gauss' algorithm?

Finite field world

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

A:

GAUSS' ALGORITHM

1. Take random $\zeta \in \mathbb{F}_q$, compute $t = \text{Order}(\zeta)$
2. If $t = q - 1$, **stop**,
3. **else** take random $\beta \in \mathbb{F}_q^*$ and compute $s = \text{Order}(\beta)$
   a. if $s = q - 1$, **stop**
   b. **else** find coprime $d \mid t$ and $e \mid s$ with $d \cdot e = \text{lcm}(t, s)$
   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

Constant-time Gauss' algorithm?

Finite field world

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

A:

GAUSS' ALGORITHM

1. Take random $\zeta \in \mathbb{F}_q$, compute $t = \text{Order}(\zeta)$
2. If $t = q - 1$, **stop**,
3. **else** take random $\beta \in \mathbb{F}_q^*$ and compute $s = \text{Order}(\beta)$
   a. if $s = q - 1$, **stop**
   b. **else** find coprime $d \mid t$ and $e \mid s$ with $d \cdot e = \text{lcm}(t, s)$
   c. set $\zeta \leftarrow \zeta^{t/d} \cdot \beta^{s/e}$ and $t \leftarrow d \cdot e$ and **repeat** from 2.

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

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

Given curve E over $\mathbb{F}_p$,
find full torsion point P
in constant-time