Generators of $\mathbb{F}_p^\times$

Recall: If $p$ is a prime number, then $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ is a field with $p$ elements. ($\Rightarrow \mathbb{F}_p$ is a finite field: [Ko])

Theorem 1: $\mathbb{F}_p^\times$ is cyclic of order $p - 1$.

Theorem 2: If $F$ is any field and $G \leq F^\times$ is a finite subgroup, then $G$ is cyclic.

Proof: The equation $x^n = 1$ has at most $n$ solutions in $F$ and hence in $G$, and so $G$ is cyclic by the criterion C4 (see overhead).

Remark: By property C1 we see that $\mathbb{F}_p^\times$ has $\phi(p - 1)$ generators. Thus, the probability that a random element $a \in \mathbb{F}_p^\times$ is a generator is:

$$P = \frac{\phi(p - 1)}{p - 1} = \prod_{q|(p-1)} \left(1 - \frac{1}{q}\right).$$

This is good if $p - 1$ has few prime factors $q$. But:

This is bad if $p - 1$ has many prime factors $q$ because

$$\prod_{q \leq n} \left(1 - \frac{1}{q}\right) \rightarrow 0, \quad \text{as } n \rightarrow \infty.$$
**Question 1:** How do we find generators of $\mathbb{F}_p^\times$?
- try: pick a random element $a \in \mathbb{F}_p^\times$.

Then we need to be able to answer:

**Question 1′:** How do we determine whether a given $a \in \mathbb{F}_p^\times$ is a generator?

**Naive Method:** Check that $a^n \neq 1$ (in $\mathbb{F}_p^\times$) for all integers $n$ with $1 \leq n < p - 1$. (Exponential!)
- Time: $O(p \log^2 p)$ (use $a^n = a^{n-1} \cdot a$).

**Better Method:** Check that $a^{(p-1)/q} \neq 1$ for all primes $q | (p - 1)$. [Justification: formula for $\text{ord}(a)$.]
- Time (to compute $a^{(p-1)/q}$) = $O(\log(\frac{p-1}{q}) \log^2 p)$
  = $O(\log^3(p))$.
- $\#P(p - 1) := \#\{q | (p - 1)\} \leq \log_2(p)$ because $p - 1 = p_1^{e_1} \cdots p_r^{e_r} \geq p_1 \cdots p_r \geq 2^r$.
- Thus: Time (Is a a generator?)
  = $O(r(f(p - 1) + \log^3(p))$
  = $O(\log(p)f(p - 1) + \log^4(p))$,
where $f(p - 1) =$ Time (to find $q | (p - 1)$)
  = $O(\exp(\sqrt{(1 + \varepsilon)\log(p)\log\log(p)})$).
→ subexponential time algorithm; cf. [Ko], p. 198.