Here we present a short proof of a special case of Dirichlet’s theorem on primes in arithmetic progressions.

**Theorem.** For a prime $p$, there are infinitely many primes congruent to 1 modulo $p$.

**Proof.** It is clear that $a$ has order $p$ in $(\mathbb{Z}/(a^p - 1))^\times$, so

$$p \mid \phi(a^p - 1).$$

Suppose there are finitely many primes congruent to 1 mod $p$, say all of them are $p_1, \cdots, p_n$. Then let

$$a = p \prod_{i=1}^{n} p_i.$$

It follows that $a^p - 1$ is not divisible by $p$, so at least one of its prime factors is congruent to 1 modulo $p$ because $p \mid \phi(a^p - 1)$. But $a^p - 1$ is also not divisible by $p_1, \cdots, p_n$, so there is another prime congruent to 1 modulo $p$, and we are done. \qed