An optimized algorithm for finding primes with (k, k')-order reciprocity

Claude Sonnet 5 (Anthropic)

August 07, 2026

Algorithm 1: RECIPROCITY(p, α_p, k, k')

Input : prime p with $p \equiv 1 \pmod{k'}$; primitive root α_p of $\mathbb{F}_p^\times$; target orders $k, k' \geq 2$
Output: all primes $q < p$ with $\mathrm{ord}_q(p) = k$ and $\mathrm{ord}_p(q) = k'$

```
Q ← ∅;
t ← (p − 1)/k' ;                                   // integer, since p ≡ 1 (mod k') is given
β ← α_p^t mod p ;                                  // ord_p(β) = k', since ord(α_p^t) = (p − 1)/ gcd(t, p − 1) = (p − 1)/t = k'
L ← {ℓ prime : ℓ | k} ;                            // maximal proper divisors of k are exactly k/ℓ, ℓ ∈ L
q ← β ;                                            // invariant: at the head of iteration s, q ≡ α_p^{st} (mod p)
for s ← 1 to k' − 1 do
    if gcd(s, k') = 1 then                         // gcd(st, p − 1) = t gcd(s, k'), so this holds iff ord_p(q) = (p − 1)/t = k' exactly
        if q ≡ 1 (mod k) and q prime then          // k | q − 1 is necessary for (ℤ/qℤ)^× to have an element of order k
            if p^k ≡ 1 (mod q) then                // necessary: forces ord_q(p) | k
                b ← true;
                for ℓ ∈ L do
                    if p^{k/ℓ} ≡ 1 (mod q) then    // ord_q(p) | k/ℓ, hence ord_q(p) < k
                        b ← false;
                        break;
                if b = true then                   // ord_q(p) | k and no maximal proper divisor works ⟹ ord_q(p) = k
                    Q ← Q ∪ {q};
    q ← q · β mod p ;                              // restores invariant: α_p^{st} · α_p^t = α_p^{(s+1)t}
return Q
```