INFINITELY MANY PRIMES WITH $(q-1, p-1)$-ORDER RECIPROCITY

For primes p, q, let $\mathrm{ord}_q(p)$ denote the multiplicative order of p modulo q. We say p and q have (k, k')-*order reciprocity* if $\mathrm{ord}_q(p) = k$ and $\mathrm{ord}_p(q) = k'$.

Theorem 1. *There exist infinitely many pairs of primes (p, q) with $(q-1, p-1)$-order reciprocity.*

The following proof is an expansion of an argument given in an answer to a question on Mathematics Stack Exchange [2].

Lemma 1. *Let p and q be odd primes with $p \equiv 1 \pmod 4$. If p is a primitive root modulo q, then q is a quadratic non-residue modulo p.*

Proof. Since p is a primitive root modulo q, $\mathrm{ord}_q(p) = q-1$. Suppose, for contradiction, that p is a quadratic residue mod q. By Euler's criterion,

$$p^{(q-1)/2} \equiv 1 \pmod q,$$

so $\mathrm{ord}_q(p) \mid \frac{q-1}{2}$, and in particular $\mathrm{ord}_q(p) \le \frac{q-1}{2} < q-1$. This contradicts $\mathrm{ord}_q(p) = q-1$. Hence p is a quadratic non-residue mod q, i.e.,

$$\left(\frac{p}{q}\right) = -1.$$

Since $p \equiv 1 \pmod 4$, quadratic reciprocity gives

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = \left(\frac{p}{q}\right) = -1,$$

so q is a quadratic non-residue modulo p. □

Lemma 2. *Let $p = 2^{2^n} + 1$ be a Fermat prime with $n \ge 1$. Then:*

(a) $p \equiv 1 \pmod 4$*;*

(b) *every quadratic non-residue mod p is a primitive root mod p.*

Proof. For (a): since $n \ge 1$, $p - 1 = 2^{2^n}$ is divisible by 4, so $p \equiv 1 \pmod 4$.

For (b): write $p - 1 = 2^s$, where $s = 2^n \ge 2$. Let a be a quadratic non-residue mod p. By Euler's criterion,

$$a^{(p-1)/2} = a^{2^{s-1}} \equiv -1 \pmod p. \tag{1}$$

Let $e = \mathrm{ord}_p(a)$. By Fermat's little theorem, $a^{p-1} \equiv 1 \pmod p$, and since $a^N \equiv 1 \pmod p$ if and only if $e \mid N$, we get $e \mid p - 1 = 2^s$; hence e is itself a power of 2, say $e = 2^k$ with $0 \le k \le s$.

If $k \le s-1$, then $e = 2^k$ divides 2^{s-1}, so $a^{2^{s-1}} \equiv 1 \pmod p$ — contradicting (1), since $p > 2$ means $1 \not\equiv -1 \pmod p$. Hence $k = s$, i.e., $e = 2^s = p - 1$, so a is a primitive root mod p. □

Proof of Theorem. A weak form of Artin's conjecture, proved unconditionally by Heath-Brown [1, Corollary 1], states that for any three distinct primes p_1, p_2, p_3, at least one of them is a primitive root modulo q for infinitely many primes q. Applying this to the three Fermat primes $5, 17, 257$, we conclude that at least one $p \in \{5, 17, 257\}$ is a primitive root modulo q for infinitely many primes q. Fix such a p, and let $\mathcal{Q}$ be the (infinite) set of primes q for which p is a primitive root mod q. Discarding the prime 2 from $\mathcal{Q}$, if present, does not affect infinitude, so we may assume every $q \in \mathcal{Q}$ is odd. By definition, $\mathrm{ord}_q(p) = q-1$ for every $q \in \mathcal{Q}$.

Fix $q \in \mathcal{Q}$. Since p is a Fermat prime, Lemma 2(a) gives $p \equiv 1 \pmod 4$, so Lemma 1 applies and shows q is a quadratic non-residue mod p. By Lemma 2(b), q is therefore a primitive root mod p, i.e. $\mathrm{ord}_p(q) = p - 1$.

Thus every $q \in \mathcal{Q}$ satisfies $\mathrm{ord}_q(p) = q - 1$ and $\mathrm{ord}_p(q) = p - 1$. As $\mathcal{Q}$ is infinite, this yields infinitely many pairs (p, q) with $(q-1, p-1)$-order reciprocity. □

References

[1] D. R. Heath-Brown, *Artin's conjecture for primitive roots*, Quart. J. Math. Oxford Ser. (2) **37** (1986), no. 145, 27–38.

[2] Answer to *Order reciprocity*, Mathematics Stack Exchange, question 3118453, answer id 3118669. `https://math.stackexchange.com/questions/3118453/order-reciprocity/3118669#3118669`