

For all r not divisible by primes p or q , find some a and b such that

$$r^{(p-1)(q-1)} - ap - bq \equiv 0 \pmod{pq}$$

Solution: First, we do some groundskeeping to tidy up the equation

$$r^{(p-1)(q-1)} \equiv ap + bq \pmod{pq} \tag{1}$$

Let's denote the left side of the equation LHS and the right side RHS. First, we work on the LHS.

Recall that the product of exponents x^{yz} can be rewritten in two forms $(x^y)^z$ and $(x^z)^y$. Hence,

$$\begin{aligned} r^{(p-1)(q-1)} &= (r^{p-1})^{q-1} \\ &= (r^{q-1})^{p-1} \end{aligned}$$

Now, we apply FLT:

$$\begin{aligned} (r^{p-1})^{q-1} &\equiv 1^{q-1} \equiv 1 \pmod{p} \\ (r^{q-1})^{p-1} &\equiv 1^{p-1} \equiv 1 \pmod{q} \end{aligned}$$

Now, we can treat the LHS as an unknown. Since p and q are prime and thus coprime, we can now apply CRT to find $r^{(p-1)(q-1)} \pmod{pq}$:

$$r^{(p-1)(q-1)} \equiv (1)pq_q^{-1} + (1)qq_p^{-1} \pmod{pq}$$

Hence, we find that $a = pq_q^{-1}$ and $b = qq_p^{-1}$ satisfies (1) for all r not divisible by p or q (here p_q^{-1} is the modular inverse of $p \pmod{q}$ and q_p^{-1} is the modular inverse of $q \pmod{p}$).