202 Final Project Proof

ceccarellim

May 2021

1 The Main Theorem and its Proof

(Euler's Theorem) Take two prime numbers, p and q. Let g be an integer,

$$g = gcd((p-1),(q-1)).$$

Then,

$$a^{(p-1)(q-1)/g} \equiv 1 \pmod{pq}, gcd(a, pq) = 1.$$

Through basic principles of modulus division, we can safely assume that g divides $p-1$, so $(p-1)/g$ has to be an integer, and that p does not divide a, so

$$a^{(p-1)(q-1)/g} = (a^{(p-1)})^{(q-1)/g}$$

Thanks to Fermat, we know that $a^{(p-1)} \equiv 1$, so we are able to replace that expression, written obviously above, with simply a 1. From here, the proof becomes very simple.

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

$$\equiv 1 \pmod{p}$$