TYPE YOUR NAME HERE
HW 26: 5.1 - 5.5
M328K
May 1st, 2012

5.1 Theorem. *If p and q are distinct prime numbers and W is a natural number with $(W, pq) = 1$, then $W^{(p-1)(q-1)} \equiv 1 \pmod{pq}$.*

Proof. □

5.2 Theorem. *Let p and q be distinct primes, k be a natural number, and W be a natural number less than pq. Then*

$$W^{1+k(p-1)(q-1)} \equiv W \pmod{pq}.$$

Proof. □

5.3 Theorem. *Let p and q be distinct primes and E be a natural number relatively prime to $(p-1)(q-1)$. Then there exist natural numbers D and y such that*

$$ED = 1 + y(p-1)(q-1).$$

Proof. □

5.4 Theorem. *Let p and q be distinct primes, W be a natural number less than pq, and E, D, and y be natural numbers such that $ED = 1 + y(p-1)(q-1)$. Then*

$$W^{ED} \equiv W \pmod{pq}.$$

Proof. □

5.5 Exercise. *Consider two distinct primes p and q. Describe every step of the RSA Public Key Coding System. State what numbers you choose to make public, what messages can be encoded, how messages should be encoded, and how messages are decoded. What number should be called the encoding exponent and what number should be called the decoding exponent?*

Solution. □