7.3 Euler's Theorem

Theorem 7.5 Euler. If $n \geq 1$ and gcd(a,n) = 1, then $a^{\phi(n)} \equiv 1 \pmod{n}$ where $\phi(n)$ is Euler's Phi-Function (Definition 7.1. For n ≥ 1, let ϕ(n) denote the number of positive integers not exceeding n that are relatively prime to n)

Ch 10 Introduction to Cryptography. From pg 204 of Elementary Number Theory, Sixth Ed. Burton

"The assumption that gcd(M,n) = 1 was made to use Euler's theorem. In the unlikely event that M and n are not relatively prime, a similar argument establishes that $r^j \equiv M \pmod{p}$ and $r^j \equiv M \pmod{q}$, which then yields the desired congruence $r^j \equiv M \pmod{n}$. We omit the details."

Question:

Given $M^k \equiv r \bmod n$ where M < n , and n = pq where p,q are distinct primes, kj ≡ 1 mod ϕ(n), and gcd(M,n) > 1, prove that $r^j \equiv M \bmod n$

$M^k \equiv r \bmod n$, thus $M^{kj} \equiv r^j \bmod n$. kj ≡ 1 mod ϕ(n) → kj = 1 + ϕ(n) L for some L ∈ $\mathbb{Z}$

If L = 0 , then kj = 1, thus $M^{kj} = M \equiv r^j \bmod n \rightarrow r^j \equiv M \bmod n$. So now let L > 0, then $M^{kj} \equiv r^j \bmod n \rightarrow r^j \equiv M^{kj} \bmod n \equiv M^{1+\phi(n)L} \bmod n \equiv M(M^{\phi(n)L}) \bmod n$. Thus we need to show that $M(M^{\phi(n)L}) \equiv M \bmod n$. gcd(M,n) > 1 and M < n implies that gcd (M,n) = p, or gcd (M, n) = q. Note if gcd(M, n) = M, then since M < n that M = p or M = q which is dealt with in the previous cases.

Now assume gcd (M,n) = p so let M = pT, for some T ∈ $\mathbb{Z}$ where T < q and gcd (T,q) = 1 since if $T \geq q$, *then* $M = pT \geq pq = n$ which contradicts M < n and if gcd (T,q) = d >1, then since only 1 | q and q | q thus d = q so q | T which contradicts T < q. Now gcd (T,q) = 1 → q doesn't divide T so by Theorem 5.1 (Fermat's Theorem) $T^{q-1} \equiv 1 \bmod q$ and $p^{q-1} \equiv 1 \bmod q$ which imply $(pT)^{q-1} \equiv 1 \bmod q$, thus since M = pT we can write $M^{q-1} \equiv 1 \bmod q \rightarrow M^{(q-1)(p-1)} \equiv 1 \bmod q$. ϕ(n) = ϕ(pq) = ϕ(p)ϕ(q) = (p-1)(q-1), thus $M^{(q-1)(p-1)} \equiv 1 \bmod q \rightarrow M^{\phi(n)} \equiv 1 \bmod q$ and $M^{\phi(n)L} \equiv 1 \bmod q \rightarrow q \mid M^{\phi(n)L} - 1 \rightarrow q \mid (M^{\phi(n)L} - 1)M$ → q | $M(M^{\phi(n)L}) - M$.
M = pT → p | M → p | $M(M^{\phi(n)L} - 1)$ → p | $M(M^{\phi(n)L}) - M$. Since p | $M(M^{\phi(n)L}) - M$ and q | $M(M^{\phi(n)L}) - M$ where gcd(p,q) = 1 then pq = n | $M(M^{\phi(n)L}) - M$, thus $M(M^{\phi(n)L}) \equiv M \bmod n$ *which* was needed. By a similar argument if gcd (M, n) = q, we can come to the same conclusion. Therefore $r^j \equiv M(M^{\phi(n)L}) \bmod n \equiv M \bmod n$