Euler's Theorem

First, we'll define a new function called the Euler phi-function or the Euler totient-function, $\phi(n)$. If n is a positive integer, then $\phi(n)$ represents the number of positive integers not exceeding n that are relatively prime to n. You should verify that $\phi(8) = 4$.

Theorem 4.1 Euler's Theorem: If m is a positive integer and a is a positive integer with $\gcd(a, m) = 1$, then $a^{\phi(n)} \equiv 1 \mod m$

1. Find $\phi(n)$ for the following integers.
   (a) 7
   The following numbers are relatively prime to 7: 1, 2, 3, 4, 5, 6. Therefore, $\phi(7) = 6$.
   (b) 10
   The following numbers are relatively prime to 10: 1, 3, 7, 9. Therefore, $\phi(10) = 4$.
   (c) 11
   The following numbers are relatively prime to 11: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10. Therefore, $\phi(11) = 10$.
   (d) 16
   The following numbers are relatively prime to 16: 1, 3, 5, 7, 9, 11, 13, 15. Therefore, $\phi(16) = 8$.
2. Find the last digit in the decimal expansion of 3^{1000}.
   We're trying to find $3^{1000} \mod 10$. $\phi(10) = 4$. $3^{1000} = (3^4)^{250} \equiv 1^{250} = 1 \mod 10$. The last digit is 1.
3. Find the last digit in the decimal expansion of $7^{999,999}$.
   $7^{999,999} = 7^{1,000,000} \times 7^{-1} = (7^4)^{250,000} \times 7^{-1}$. We're still in mod 10, so $(7^4)^{250,000} \times 7^{-1} \equiv 1^{250,000} \times 7^{-1} = 1 \times 7^{-1} = 7^{-1}$. By iterating from numbers 1 to 7, I found that the multiplicative inverse of 7 mod 10 is 3, so the last digit is 3.
4. Find the number in $\mathbb{Z}_{35}$ congruent to $3^{100,000}$.
   The following numbers are relatively prime to 35: 1, 2, 3, 4, 6, 8, 9, 11, 12, 13, 16, 17, 18, 19, 22, 23, 24, 26, 27, 29, 31, 32, 33, 34. Thus, $\phi(35) = 24$. $3^{100,000} = (3^{24})^{4000} \times 3^{4000} \equiv 1^{4000} \times 3^{4000} = 3^{4000} = (3^{24})^{160} \times 3^{160} \equiv 1^{160} \times 3^{160} = (3^{24})^6 \times 3^{16} \equiv 1^6 \times 3^{16} = (3^5)^3 \times 3 = 243^3 \times 3 \equiv (-2)^3 \times 3 = -24 \equiv 11 \mod 35$. Thus, $3^{100,000} \equiv 11 \mod 35$.
5. Use Euler's Theorem to find the multiplicative inverse of 2 modulo 9.
   9 is relatively prime to: 1, 2, 4, 5, 7, 8. $\phi(9) = 6$. Therefore, $2^6 = 2 \times 2^5 \equiv 1 \mod 9$. Therefore, the multiplicative inverse of 2 mod 9 is 2^5. $2^5 = 32 \equiv 5$, so 5 is the multiplicative inverse of 2 modulo 9.
6. Solve each of the following linear congruences using Euler's Theorem.
   (a) $5x \equiv 3 \mod 14$
   $x = 5^{-1} \times 3 \mod 14$. 14 is relatively prime to: 1, 3, 5, 9, 11, 13. Therefore, $\phi(14) = 6$, so $5^6 \equiv 1 \mod 14$, so $5^{-1} \equiv 5^5 \mod 14$. $5^5 = 25 \times 25 \times 5 \equiv -3 \times -3 \times 5 = 45 \equiv 3$. So, $5^{-1} \equiv 3 \mod 14$, so $x = 3 \times 3 = 9$.
   (b) $4x \equiv 7 \mod 15$
   $x = 4^{-1} \times 7 \mod 15$. 15 is relatively prime to: 1, 2, 4, 7, 8, 11, 13, 14. Therefore, $\phi(15) = 8$, so the multiplicative inverse of 4 modulo 15 is 4^7. $4^7 = (4^2)^3 \times 4 = 16^3 \times 4 \equiv 1^3 \times 4 = 4$. Therefore, $x = 4 \times 7 = 28 \equiv 13 \mod 15$. $x = 13$.
   (c) $3x \equiv 5 \mod 16$
   $x = 3^{-1} \times 5 \mod 16$. 16 is relatively prime to: 1, 3, 5, 7, 9, 11, 13, 15. Therefore, $\phi(16) = 8$, so the multiplicative inverse of 3 modulo 16 is 3^7. $3^7 = 3^3 \times 3^3 \times 3 = 27 \times 27 \times 3 \equiv 11 \times 11 \times 3 = 11 \times 33 \equiv 11 \times 1 = 11$. $x = 11 \times 5 = 55 \equiv 7 \mod 16$. $x = 7$.
7. If p and q are distinct primes, what is $\phi(pq)$? It is safe to assume that ϕ is a multiplicative function (i.e., $\phi(pq) = \phi(p) \cdot \phi(q)$) if p and q are distinct primes.
   Because p is prime, only 1 and p divide it evenly. Thus, for every number n such that $0 < n < p$, $\gcd(n, p) = 1$. n can be any integer in the range $[1, p-1]$, so there are $p-1$ numbers less than and relatively prime to p, so $\phi(p) = p - 1$. By the same reasoning, $\phi(q) = q - 1$. Since ϕ is multiplicative, $\phi(pq) = \phi(p) \cdot \phi(q) = (p-1)(q-1)$.