Cryptology Packet Pt4

ID: 1747

January 2023

1. Find $\phi(n)$ for the following integers.
   (a) 7

       7 is relatively prime to $1, 2, 3, 4, 5, 6$
       $\phi(7) = 6$
   (b) 10

       10 is relatively prime to $1, 3, 7, 9$
       $\phi(10) = 4$
   (c) 11

       11 is relatively prime to $1, 2, 3, 4, 5, 6, 7, 8, 9, 10$
       $\phi(11) = 10$
   (d) 16

       16 is relatively prime to $1, 3, 5, 7, 9, 11, 13, 15$
       $\phi(16) = 8$

2. Find the last digit in the decimal expansion of 3^{1000}.

   $3^{1000} \mod 10$
   $\phi(10) = 4$
   $3^4 \equiv 1 \mod 10$
   $81 \mod 10 \equiv 1$

3. Find the last digit in the decimal expansion of $7^{999,999}$

   $7^{999,999} \mod 10$
   $\phi(10) = 4$
   $7^4 \equiv 1 \mod 10$
   $49 * 49 \equiv 1 \mod 10$
   $49 * 49 \mod 10 \equiv 1$

4. Find the number in $\mathbb{Z}_{35}$ congruent to $3^{100,000}$

$3^{100,000} \equiv \mod 35$
$3^{\phi(35)} \equiv 1 \mod 35$
$\phi(35) = 25$
$3^{25} \equiv 1 \mod 35$
$3^{25} \mod 35 \equiv 1$
$3^{25} \mod 35 \equiv 1$

5. Use Euler's Theorem to find the multiplicative inverse of 2 modulo 9.

   $2^{\phi(9)} \equiv 1 \mod 9$
   $\phi(9) = 6$
   $2^6 \equiv 1 \mod 9$
   $2^5 * 2^1 \equiv 1 \mod 9$
   $2^5 \equiv 5 \mod 9$

6. Solve each of the following learn congruences using Euler's Theorem.

   (a) $5x \equiv 3 \mod 14$

   $5^{\phi(14)} \equiv 1 \mod 14$
   $5^6 \equiv 1 \mod 14$
   $5x \equiv 3 \mod 14$
   $5x \equiv 1 * 3 \mod 14$
   $5x \equiv 3 * 5^6 \mod 14$
   $5x \equiv 3 * 5 * 5^5 \mod 14$
   $x \equiv 3 * 5^5 \mod 14$
   $x \equiv 3 * 25 * 5^3 \mod 14$
   $x \equiv 3 * 11 * 5^3 \mod 14$
   $x \equiv 3 * 11 * 25 * 5 \mod 14$
   $x \equiv 3 * 11 * 11 * 5 \mod 14$
   $x \equiv 3 * 11 * 13 \mod 14$
   $x \equiv 3 * 3 \mod 14$
   $x \equiv 9 \mod 14$

   (b) $4x \equiv 7 \mod 15$

   $4^{\phi(15)} \equiv 1 \mod 15$
   $4^8 \equiv 1 \mod 15$
   $4x \equiv 7 * 4^8 \mod 15$
   $4x \equiv 7 * 4^8 \mod 15$
   $x \equiv 7 * 4^7 \mod 15$
   $x \equiv 7 * 256 * 4^3 \mod 15$
   $x \equiv 7 * 4 \mod 15$
   $x = 13$

   (c) $3x \equiv 5 \mod 16$

   $3^{\phi(16)} \equiv 1 \mod 16$

$3^8 \equiv 1 \mod 16$
$3x \equiv 5 * 1 \mod 16$
$3x \equiv 5 * 3^8 \mod 16$
$3x \equiv 45 * 3^6 \mod 16$
$3x \equiv 13 * 3^6 \mod 16$
$x \equiv 13 * 3^5 \mod 16$
$x \equiv 13 * 11 * 3^2 \mod 16$
$x \equiv 15 * 3^2 \mod 16$
$x \equiv 13 * 3 \mod 16$
$x \equiv 7 \mod 16$

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., $\phi(pq) = \phi(p) * \phi(q)$) if p and q are distinct primes.

   $\phi(p) = p - 1$ bc p is prime
   $\phi(q) = q - 1$ bc q is prime
   $\phi(pq) = \phi(p) * \phi(q)$ so $\phi(pq) = (p - 1)(q - 1)$