Cryptology 4

Ryan Kellar

February 2024

1 Problem 1

1.1 a)

6

1.2 b)

4

1.3 c)

10

1.4 d)

8

2 Problem 2

1

3 Problem 3

3

4 Problem 4

11

5 Problem 5

$2k \bmod 9 = 1$
$\phi(9) = 6$
$2^6 \bmod 9 = 1$
$2 * 2^5 \bmod 9 = 1$
$= 32$ (However, this is not in $\mathbb{Z}_3 2$)
$32 \bmod 9 = 5$

6 Problem 6

6.1 a)

$5x \bmod 14 = 3$
$x \bmod 14 = 3 * 3$ (3 is the multiplicative inverse of 5 in mod 14)
$x \bmod 14 = 9$
$x = 9$

6.2 b)

$4x \bmod 15 = 7$
$x \bmod 15 = 7 * 4$ (4 is the multiplicative inverse of 4 in mod 15)
$x \bmod 15 = 28$
$x = 28 \bmod 15$
$x = 13$

6.3 c)

$3x \bmod 16 = 5$
$x \bmod 16 = 5 * 5.6667$ (5.6667 is APPROXIMATELY the multiplicative inverse of 3 in mod 16)
$x \bmod 16 = 28.3333$
$x = 28.3333 \bmod 16$
$x = 12.3333$

7 Problem 7

If p and q are primes, that means that $\phi(p) = p - 1$ (by definition of Euler's totient function), and therefore $\phi(q) = q - 1$ as well, since for both p and q all of $\forall x | x \in \mathbb{Z}_p$ each factor will be coprime with p (or q).
Since we can assume that $\phi(x)$ is a multiplicative function, that means $\phi(pq) = \phi(p) * \phi(q)$. Using the identity I stated earlier, we can also re-write this as $(p - 1)(q - 1)$, or in polynomial form, $pq - p - q + 1$.