HW #5 - CNS Sapienza

Daniele Oriana 1457625

10 Dec 2015

20150114-Q5

Miscellaneous
Provide short answers (2 lines max) to the following questions.
Q5.1 [1/30] $\Phi(7) = ?$ (Φ is the Euler's totient function)
Q5.2 [1/30] $\Phi(12) = ?$
Q5.3 [2/30] Find the multiplicative inverse of 5 (mod 6)
Q5.4 [1/30] Define the birthday bound
Q5.5 [2/30] Is weak resistance to collisions implying strong resistance?

Answer

Q5.1

$\Phi(7)=6$ we have to note that for a prime number we obtain $\Phi(n)=n-1$.

Q5.2

$\Phi(12)=\#\{1,5,7,11\}=4$ because these numbers are the only ones, smaller then 12, that are coprime with 12.

Q5.3

The multiplicative inverse of 5 (mod 6) is 5, in fact we have that x is the multiplicative inverse of a if $a \cdot x \equiv 1 \bmod n$ by definition, so with 5 we have that $5 \cdot 5 = 25 = 1 \bmod 6$.

Q5.4

The birthday bound is the approximative number of attempts to generate a collision using brute force.

Q5.5

No, because the "strong class" is a subset of the "weak class", we can see it from the difference between the two definitions where the definition of weak resistance is bounded to a particular choice of one element, while the definition of strong resistance is more general.