MATH 1025: Introduction to Cryptography

# Bonus 3

crazy frog

**Problem 1.** How many solutions (modulo $n$) does the congruence $x^2 \equiv 1 \pmod{n}$ have?

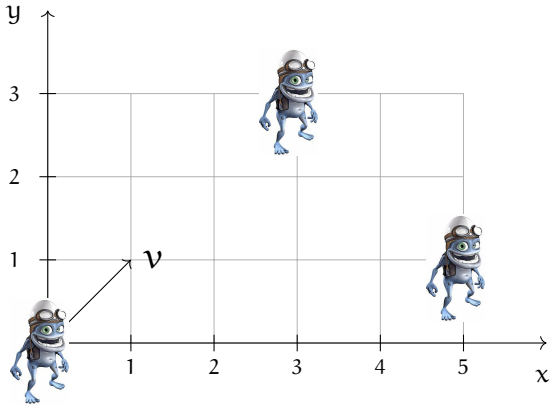
(a) [1 **pt**] $n = pq$ with $p$ and $q$ odd primes;

(b) [1 **pt**] $n = 2p$ with $p$ odd prime;

(c) [2 **pt**] $n = p_1 p_2 \dots p_k$ with all $p_i$'s being pairwise different odd prime numbers.

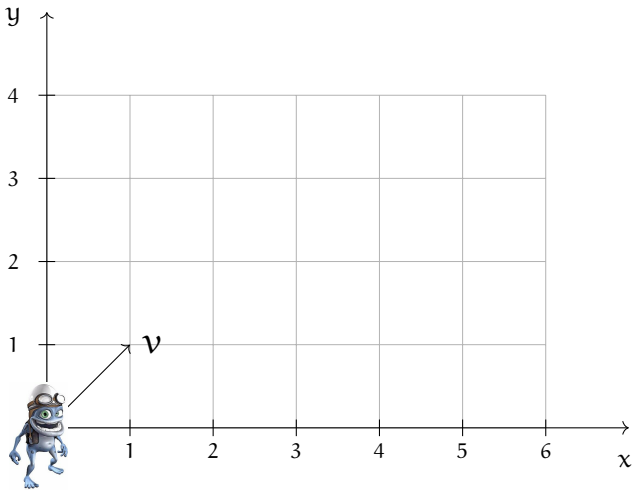
**Problem 2.** The Crazy Frog[1] jumps on the rectangular grid according to the following rule: from point $(a, b)$ he jumps to the point $(a+1 \pmod m, b+1 \pmod n)$. For each of the examples below answer the following questions. Assuming the frog is at the origin, will he be able to visit all other points on the rectangular grid? Would your answer change if the starting point is any other point $(a, b)$? (Give an explanation)

(a) [1 **pt**] $(m, n) = (6, 4)$




[1] Crazy Frog, originally known as The Annoying Thing, is a Swedish CGI-animated character and musician created in 2003 by actor and playwright Erik Wernquist.

(b) [2 **pts**] $(m, n) = (7, 5)$



(c) [3 **pts**] Now let $(m, n) \in \mathbb{Z}_{>1} \times \mathbb{Z}_{>1}$ be arbitrary numbers. How many vertices inside the $(m \times n)$-rectangle will the frog be able to visit?[2] What is the condition on $(m, n)$, so that he visits all grid points inside the rectangle?

[2] The answer is a simple expression in $m$ and $n$.