MATH 1025: Introduction to Cryptography

Homework 2

ring of arithmetic

Problem 1. Find the orders of the multiplicative groups[1]

(a) [5 **pts**] $(\mathbb{Z}/37\mathbb{Z})^{\times}$.

(b) [5 **pts**] $(\mathbb{Z}/20\mathbb{Z})^{\times}$.

Problem 2. Find solutions of the following congruences [2]

(a) [5 **pts**] $33x + 12 \equiv 48 \pmod 5$

[1]**Hint:** the number of elements in $(\mathbb{Z}/m\mathbb{Z})^{\times}$ is equal to the number of elements $0 < a \leq m - 1$, coprime to m.
[2]**Hint:** if you can't figure out a clever way to find the solution(s), just substitute each value $x = 1, x = 2, \ldots, x = m - 1$ and see which ones work.

(b) [5 **pts**] $x^2 \equiv 3 \pmod{11}$

(c) [5 **pts**] $x^2 \equiv 1 \pmod{8}$

Problem 3**.** Find a single value x that simultaneously solves the two congruences:

(a) [10 **pts**] $x \equiv 3 \pmod{7}$ and $x \equiv 4 \pmod{9}$ [3]

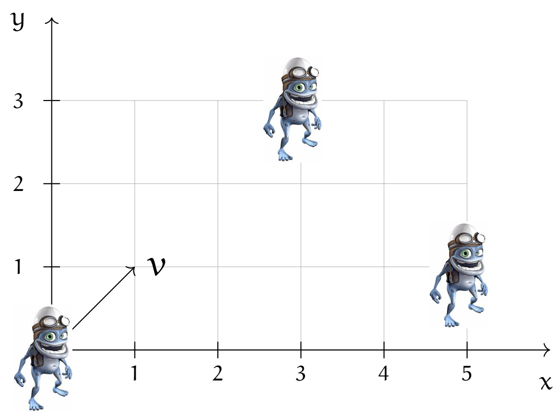
(b) [10 **pts**] $x \equiv 4 \pmod{7}$ and $x \equiv 5 \pmod{8}$

[3]**Hint:** note that every solution of the first congruence looks like $x = 3 + 7y$ for some y. Substitute this into the second congruence and solve for y; then use that to get x.

Problem 4. Crazy Frog[4] jumps on 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 starts at the origin

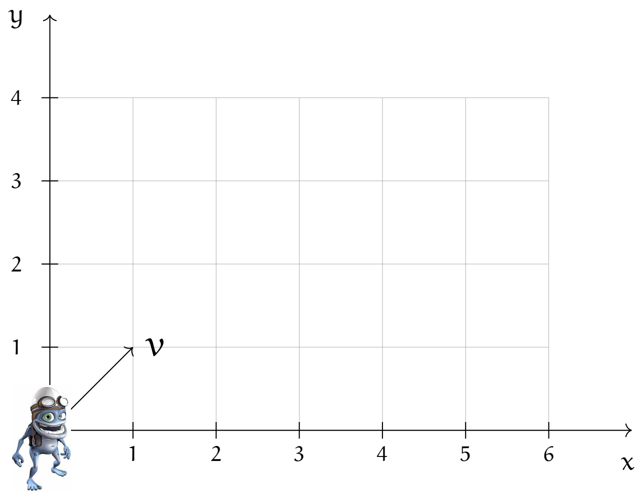
- give the list of the points he will 'visit' (jump on) prior to returning;
- answer the questions: will he visit all points on the rectangular grid? Would your answer change if the starting point was any other point (a, b)? (explain)

(a) [5 **pts**] $(m, n) = (6, 4)$



[4]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) [5 **pts**] $(m, n) = (7, 5)$



(c) [15 **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?[5] What is the condition on (m, n), so that he visits all grid points inside the rectangle?

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

Baby-step giant-step algorithm

Problem 5. Consider the multiplicative group $(\mathbb{Z}/13\mathbb{Z})^\times$ and elements $g = 7, h = 4$ in it.

(a) [5 **pts**] Find the order N of g.

(b) [5 **pts**] Write down the elements of lists L_1 and L_2.

(c) [5 **pts**] Pick an element in the intersection $L_1 \cap L_2$ and use it to find s with $7^s = 4$.

Pohlig-Hellman algorithm

Problem 6. Again, we will work the multiplicative group $(\mathbb{Z}/13\mathbb{Z})^\times$ and elements $g = 7, h = 4$ in it.

(a) [5 **pts**] Write the order N of g as the minimal product of pairwise coprime positive integers. Use this factorization and CRT to write the cyclic group $\langle g \rangle \simeq \mathbb{Z}/N\mathbb{Z}$ as a product of cyclic groups of smaller order.

(b) [5 **pts**] Your answer in (a) should be a product of two groups. Find the corresponding pairs of elements (g_1, g_2) and (h_1, h_2).

(c) [5 **pts**] Write down the system of two congruences $\begin{cases} g_1^{s_1} \equiv h_1 \pmod{13} \\ g_2^{s_2} \equiv h_2 \pmod{13} \end{cases}$ and use it to deduce the system of congruences on (s_1, s_2) (here $N = n_1 \cdot n_2$ is the decomposition that you obtained in (a)). Then find s as the solution of the system.