Pruebas de Conocimiento Cero y sus Aplicaciones

José Luis Cánovas Sánchez

Tutores:
Antonio José Pallarés Ruiz
Leandro Marín Muñoz

8 de julio de 2017

Universidad de Murcia
Facultad de Matemáticas

Outline

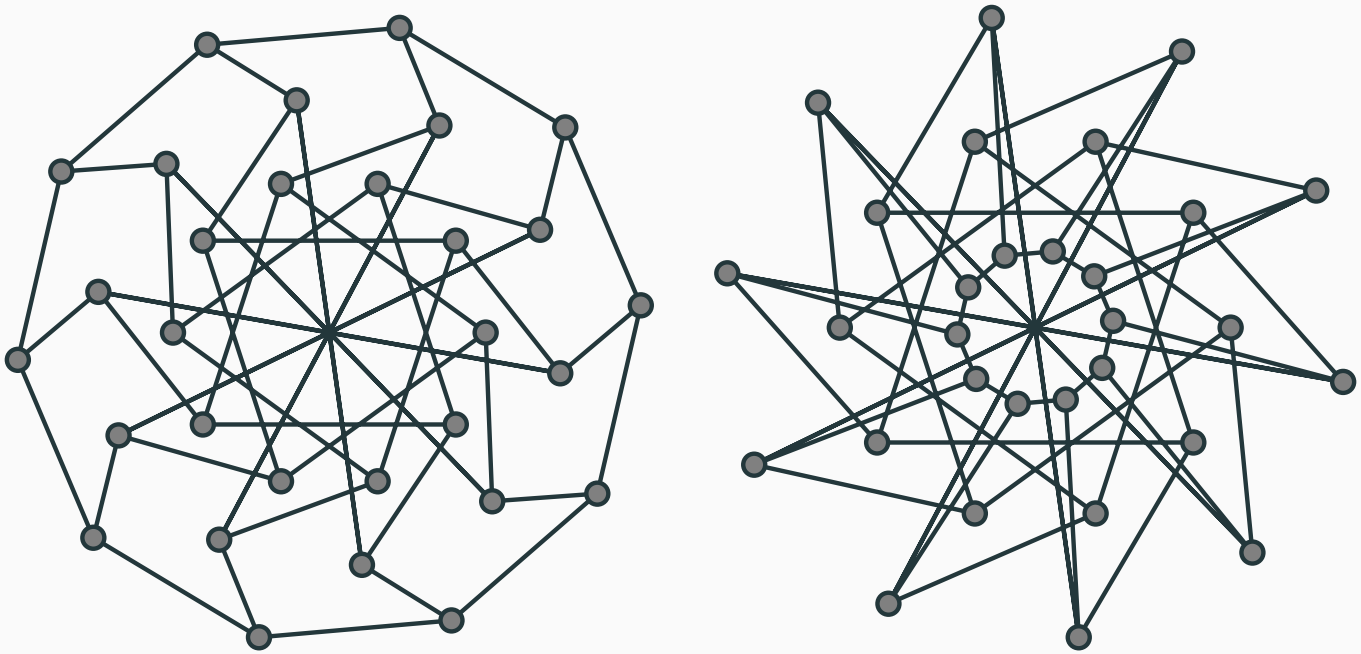
Problems

Graph Isomorphism

Name Graph Isomorphism Problem (GI).

Instance Given two graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ with $\mid V_1 \mid = \mid V_2 \mid = n$.

Question Is there a permutation $\tau : V_1 \to V_2$ such that an edge $(u, v) \in E_1$ if and only if $(\tau(u), \tau(v)) \in E_2$?

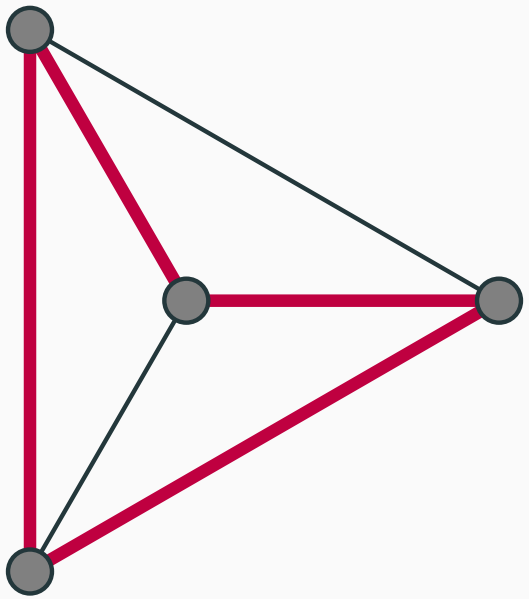


Hamiltonian Cycle $^{\text{NPC}}$

Name Hamiltonian Cycle Problem (HC).

Instance Given graph $G = (V, E)$.

Question Does there exist a Hamiltonian cycle in G?

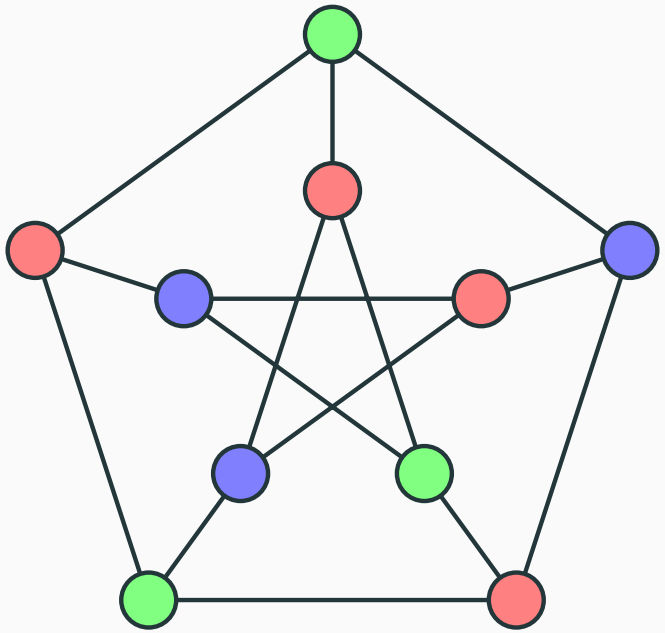


Graph 3-colorability NPC

Name Graph 3-colorability Problem (G3C).

Instance Given graph $G = (V, E)$.

Question Is there a function $\phi : V \to \{1, 2, 3\}$ such that $\phi(u) \neq \phi(v) \quad \forall (u, v) \in E$?



Quadratic residue

Name Factorization problem (FACT).

Instance Positive integer N.

Question Are there integers $p, q \geq 2$ such that $N = pq$?

Name Quadratic residue problem (QR).

Instance Given a composite integer $N = pq$ and the integer x with Jacobi Symbol $\left(\frac{x}{N}\right) = 1$.

Question Is x a quadratic residue in $\mathbb{Z}_N$? $\exists a \in \mathbb{Z}_N : x \equiv a^2 (N)$?

Theorem

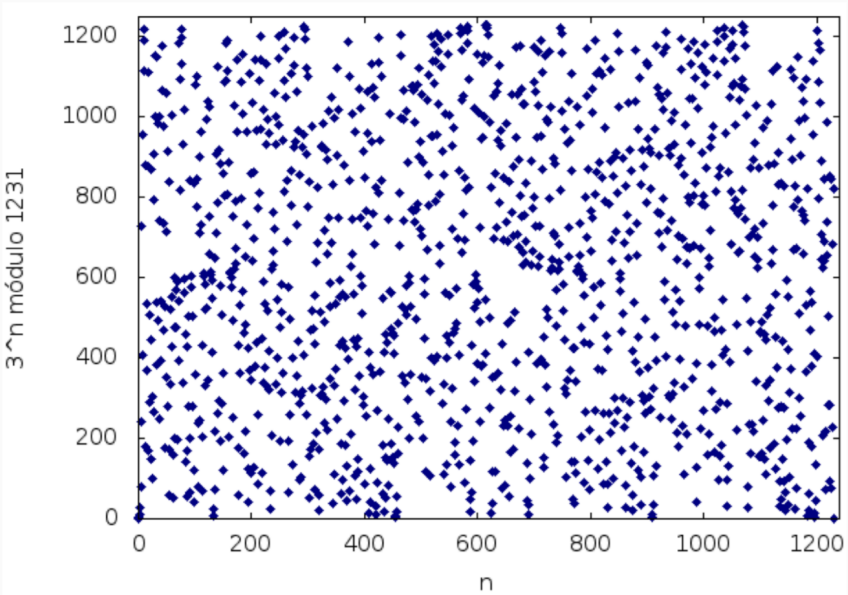
$QR \leq_P FACT$

Discrete Logarithm

Name Discrete Logarithm problem (DL).

Instance A cyclic group $G = \langle g \rangle$ of prime order q, an element $y \in G$.

Question What is the integer $s \in \mathbb{Z}_q$ such that $g^s = y$, or $log_g y = s$?



Discrete Logarithm with $G = \mathbb{Z}_{1231}$, $g = 3$.

Adolfo Quirós Gracián. *Grupos y criptografía: de Julio César a las curvas elípticas.*

Pruebas Interactivas