Exercise 1 [11 points] Given an undirected graph $G = (V, E)$ and a positive integer $k \geq 2$, a *k-multicut* is a partition of V into k disjoint subsets $V_1, V_2, \ldots, V_k$, with $\bigcup_{i=1}^{k} V_i = V$ and $V_i \cap V_j = \emptyset$, for $1 \leq i \neq j \leq k$ (observe that the V_i's may be empty). The *cardinality* $S(V_1, V_2, \ldots, V_k)$ of the k-multicut is defined as the number of edges of E whose endpoints belong to distinct subsets of the partition, that is:

$$S(V_1, V_2, \ldots, V_k) = |\{e = \{u, v\} \in E : \exists 1 \leq i \neq j \leq k : (u \in V_i) \wedge (v \in V_j)\}|.$$

Given $G = (V, E)$ and $k \geq 2$, consider the problem of determining a k-multicut di G of maximum cardinality. Provide the pseudocode and analyze a randomized approximation algorithm APPROX-MULTICUT$(G = (V, E), k)$ for the problem, and study its approximation factor ρ as a function of k.

APPROX_MULTICUT $(G=(V,E), k)$: // $k \in [2, |V|]$
  foreach $v \in V$ do:
    $p[v] \leftarrow$ RANDOM$(\{1, \ldots, k\})$.
  $V_i : \{v \in V : p[v] = i\}$
  return $(V_1, \ldots, V_k)$;

$T_{AM}(n, m) = O(n)$

$\rho = \frac{S(V_1^*, \ldots, V_k^*)}{\mathbb{E}[S(V_1, \ldots, V_k)]}$

$\forall e \in E$, X_e r.v. : $X_e = 1$ iff "$e = \{u, v\}$ is cut-edge (attraversa partizioni)

$\Pr[X_e = 1] = \mathbb{E}[X_e] = 1 - \Pr[X_e = 0] = 1 - \Pr[p[u] = p[v]] = 1 - \frac{k}{k^2} = 1 - 1/k \to 1$ per $k \to +\infty$

$\mathbb{E}[S(V_1, \ldots, V_k)] = \mathbb{E}\left[\sum_{e \in E} X_e\right] = \sum_{e \in E} \mathbb{E}[X_e] = \sum_{e \in E} (1 - 1/k) = m\frac{k-1}{k}$

$\rho \leq \frac{m}{m\frac{k-1}{k}} = \frac{k}{k-1}$

Exercise 2 [10 points] Let a, b, c be three positive integers. Show that

$$\max\{\gcd(a,b), \gcd(a,c)\} \leq \gcd(a, b \cdot c) \leq \gcd(a,b) \cdot \gcd(a,c).$$

($\leq$) $\gcd(a,b) \mid b \Rightarrow \exists k_1 : k_1 \cdot \gcd(a,b) = b \Rightarrow bc = \underbrace{k_1 c}_{k_2} \gcd(a,b) \Rightarrow$

$\Rightarrow bc = k_2 \gcd(a,b) \Rightarrow \begin{cases} \gcd(a,b) \mid bc \\ \gcd(a,b) \mid a \end{cases} \Rightarrow \gcd(a,b)$: comun divisore $\Rightarrow$
di bc, a

$\Rightarrow \gcd(a,b) \leq \gcd(a, bc) \Rightarrow$ simmetria: $\gcd(a,b) \leq \gcd(a,bc) \Rightarrow$
$\Rightarrow \max\{\gcd(a,b), \gcd(a,c)\} \leq \gcd(a,bc)$

($\geq$) Bezout:
$\exists x_1, y_1 : \gcd(a,b) = a x_1 + b y_1 \quad \exists x_2, y_2 : \gcd(a,c) = a x_2 + c y_2 \Rightarrow$
$\Rightarrow \gcd(a,b)\gcd(a,c) = (a x_1 + b y_1)(a x_2 + c y_2) = a \underbrace{(a x_1 x_2 + c x_1 y_2 + b y_1 x_2)}_{\bar{x}} +$
$+ bc \underbrace{y_1 y_2}_{\bar{y}} = a\bar{x} + bc\bar{y}$

Bezout: $\gcd(a, bc) \leq \gcd(a,b)\gcd(a,c)$

Exercise 3 [11 points] Let o_1, o_2, o_3 be three objects. Design a randomized routine R3(o_1, o_2, o_3) that uses exclusively RANDOM$(\{0,1\})$ as a source of randomness and returns every $o_i, 1 \leq i \leq 3$, with probability $1/3$. Prove the correctness of R3(o_1, o_2, o_3) and determine the average number of calls to RANDOM$(\{0,1\})$ performed by R3.

```
R3(o1, o2, o3):
while true:
    b0 ← RANDOM(0,1);
    b1 ← RANDOM(0,1);
    // sia i: (i)_2 = b1 b0
    (i ← 2b1 + b0)
    if i > 0: return oi
```

111
222
333

Correttezza:
total prob.
E_i = "R_3 termina con o_i" $\forall i \geq 1 \Rightarrow$ copre Ω
$\Pr[\bigcup_{i \geq 1} E_i] = 1, \quad E_i \cap E_j = \emptyset$

$$\forall i \in [1,3]: \Pr[R_3(o_1, o_2, o_3) = o_i] = \sum_{j=1}^{\infty} \Pr(o_1, o_2, o_3 \mid E_j) \Pr[E_j] =$$

$$= \frac{1}{3} \sum_{j=1}^{\infty} \Pr[E_j] = 1/3$$

chiamate a RANDOM
return a o_i con prob. $1 \cdot 1/4 = 3/4 \Rightarrow$ #chiamate $\sim$ Geom$(\frac{3}{4}) \Rightarrow$

$\#$ it. $= 4/3 \Rightarrow \mathbb{E}[\#\text{chiamate}] \leq 2 \cdot \frac{4}{3} = \frac{8}{3} < 3$

Esercizio 1 [11 pts] Consider the following decision problem:

MAJORITY-SAT

ISTANCE: $\langle \Phi(x_1, x_2, \ldots, x_n) \rangle$,
Φ boolean formula, $n > 0$.

QUESTION: Is Φ satisfied by at least a majority (e.g., $\geq 2^{n-1} + 1$)
of all possible truth assignments to the n variables?

Show that MAJORITY-SAT is NP-Hard (*Hint*: Reduce from SAT, trying to "amplify" the number of satisfying assignments of a formula)

$\langle \phi(x_1,\ldots,x_n) \rangle \in SAT \Rightarrow \exists \vec{b} \in \{0,1\}^n : \phi(\vec{b}) = 1$

$\langle \phi(x_1,\ldots,x_n) \rangle \Rightarrow$ aggiungiamo variabili $\Rightarrow \phi'(x_1,\ldots,x_n,x_{n+1}) = \phi(x_1,\ldots,x_n) \vee x_{n+1} \Rightarrow$ ($N = n+1$)
$\Rightarrow$ # satisfying assignments sotto $b_{n+1} = 1 : 2^n = 2^{N-1} \Rightarrow$ poi ho altro $\vec{b}$ da $\phi \in SAT$

Riduzione:
$f: \langle \phi(x_1,\ldots,x_n) \rangle \rightsquigarrow \langle \phi'(x_1,\ldots,x_n,x_{n+1}) \rangle = \langle \phi(x_1,\ldots,x_n) \vee x_{n+1} \rangle \Rightarrow$ etc

Dimostriamo $\langle \phi \rangle \in SAT \leftrightarrow f(\langle \phi \rangle) \in M\_SAT$

($\rightarrow$) $\langle \phi \rangle \in SAT \Rightarrow \exists \vec{b} \in \{0,1\}^n : \phi(\vec{b}) = 1 \Rightarrow \forall b \in \{0,1\}^n \ (\vec{b}, 1)$ soddisfa $\phi' \Rightarrow$
$\Rightarrow$ sono $2^n = 2^{N-1}$, $(\vec{b}, 0)$ soddisfa $\Rightarrow \geq 2^{N-1} + 1$ satisfying assignments per ϕ'

($\leftarrow$) $\langle \phi' \rangle \in M\_SAT \Rightarrow \exists \geq 2^{(n+1)-1} + 1$ satisfying per $\phi' \Rightarrow$ ho solo $2^{(N+1)-1} = 2^n$
ass. con $b_{n+1} = 1 \Rightarrow \exists$ ass. $\vec{b} = (\vec{b}, 0)$ satisfying $\phi' \Rightarrow \phi'(\vec{b}) = \phi(\vec{b}) \vee 0$:
deve avere $\phi(\vec{b}) = 1 \Rightarrow \langle \phi \rangle \in SAT$

Esercizio 2 [10 pts] Determine $(43)^{-1}$ in $\boldsymbol{Z}^*_{243}$. All passages of the computation process have to be reported in your solution.

$(43)^{-1} \in \mathbb{Z}^*_{243}$

EE(243, 43) → EE(43, 28) → EE(28, 15) → EE(15, 13) → EE(13, 2) → EE(2, 1) → EE(1, 0) ⟶ {1, (1, 0)}

{1, (0, 1)} ↑ {1, (1, −6)} ↑ {1, (−6, 7)} ↑ ⋮ ↑ {1, (130, −113)}

$43^{-1} = -113 \bmod 243$

$(x', y') \to (y', x' - \lfloor \frac{a}{b} \rfloor y')$

Esercizio 3 [11 pts] Let n and k be two integer parameters, with $n > 2$ and $0 < k < n$. Consider n numbered boxes, $b_1, b_2, \ldots, b_n$, and an experiment where $m > 0$ indistinguishable balls are thrown independently and randomly into these n boxes. Determine a lower bound on m (as a function f of parameters n and k) such that for $m \geq f(n,k)$, with probability at least $1 - 1/n$ there are no k consecutively numbered empty boxes. (*Hint:* the union bound might be useful).

Fissiamo sequenza arbitraria di bins $b_j, \ldots, b_{j+k-1}$, $j \in [1, n-k+1]$

$n-k$ tali sequenze possibili

$\Pr[\text{"bins } b_j, \ldots, b_{j+k-1} \text{ tutti vuoti"}] = \frac{(n-k)^m}{n^m} = \left(1 - \frac{k}{n}\right)^m$

Scegliamo $\bar{m}$ per rendere prob. molto piccola ($\leq 1/n^2$)

$\left(1 - \frac{k}{n}\right)^{\bar{m}} = \left(1 - \frac{k}{n}\right)^{\frac{n}{k}\frac{k}{n}\bar{m}} < e^{-\frac{k}{n}\bar{m}} = 1/n^2 \Rightarrow$ basta $\frac{k}{n}\bar{m} = 2\ln 2 \Rightarrow$

$\Rightarrow \bar{m} = \lceil \frac{n}{k} 2 \ln n \rceil \Rightarrow \Pr[\text{"qualche seq. vuota"}] \leq n \frac{1}{n^2} = 1/n$