The COLOURABILITY problem.
Instance: An undirected graph $G$, and an integer $k$.
QUESTION: Is there an assignment of $k$ colours to the vertices of $G$ such that no two adjacent vertices receive the same colour?

THEOREM COLOURABILITY is NP-complete.

Reduction from Sat to COLOURABILITY.

Given: $\phi$, instance of SAT, i.e., a Boolean formula in CNF.

Require: Graph $G$ and integer $k$ s.t.
$\phi$ is satisfiable $\Longleftrightarrow G$ is $k$-colourable.

Formally: Let

$$
\begin{array}{ll}
x_{1}, x_{2}, \ldots, x_{n}: & \text { variables in } \phi, \\
C_{1}, C_{2}, \ldots, C_{r}: & \text { clauses of } \phi .
\end{array}
$$

## Then

$$
\begin{aligned}
V= & \left\{v_{0}, \ldots, v_{n}\right\} \cup\left\{x_{1}, \ldots, x_{n}\right\} \cup\left\{\bar{x}_{1}, \ldots, \bar{x}_{n}\right\} \\
& \cup\left\{C_{1}, \ldots, C_{r}\right\}, \\
E= & \left\{\left\{v_{i}, x_{j}\right\},\left\{v_{i}, \bar{x}_{j}\right\} \mid 1 \leq i, j \leq n \text { and } i \neq j\right\} \\
& \cup\left\{\left\{v_{i}, v_{j}\right\} \mid 0 \leq i<j \leq n\right\} \\
& \cup\left\{\left\{v_{0}, C_{k}\right\} \mid 1 \leq k \leq r\right\} \\
& \cup\left\{\left\{x_{i}, \bar{x}_{i}\right\} \mid 1 \leq i \leq n\right\} \\
& \cup\left\{\left\{x_{i}, C_{k}\right\} \mid x_{i} \text { is not a literal in clause } C_{k}\right\} \\
& \cup\left\{\left\{\bar{x}_{i}, C_{k}\right\} \mid \neg x_{i} \text { is not a literal in clause } C_{k}\right\}, \\
k= & n+1 .
\end{aligned}
$$

The Integer Programming problem, INTPROG.

INSTANCE: An integer $m \times n$ matrix $A$, and an integer $m$-vector $\mathbf{b}$.
QUESTION: Does there exist an integer $n$-vector $\mathbf{x}$ such that $A \mathrm{x} \leq \mathrm{b}$ ?

## THEOREM INTPROG is NP-complete.

Note: INTPROG is in NP but tricky to show!

NP-hardness: Reduction from SAT to INTPROG.

Formally: Let

$$
\begin{array}{ll}
x_{1}, x_{2}, \ldots, x_{n}: & \text { variables in } \phi, \\
C_{1}, C_{2}, \ldots, C_{r}: & \text { clauses of } \phi .
\end{array}
$$

Then for $1 \leq i \leq r$ and $1 \leq j \leq n$ define

$$
\alpha_{i j}= \begin{cases}1, & \text { if } x_{j} \text { occurs in the clause } C_{i} ; \\ 0, & \text { otherwise }\end{cases}
$$

and

$$
\beta_{i j}= \begin{cases}1, & \text { if } \neg x_{j} \text { occurs in the clause } C_{i} ; \\ 0, & \text { otherwise. }\end{cases}
$$

Let $z_{1}, z_{2}, \ldots, z_{n}$ be integer variables and consider linear inequalities:

$$
\begin{aligned}
z_{j} \geq 0, & \text { for } 1 \leq j \leq n \\
z_{j} \leq 1, & \text { for } 1 \leq j \leq n \\
\sum_{j=1}^{n}\left(\alpha_{i j} z_{j}+\beta_{i j}\left(1-z_{j}\right)\right) \geq 1, & \text { for } 1 \leq i \leq r
\end{aligned}
$$

The Subsetsum problem.
INSTANCE: A finite set $X$, a positive integer ‘size' $s(x)$ for each $x \in X$, and an integer ‘goal' b.
Question: Is there a subset $A \subseteq X$ such that $\sum_{x \in A} s(x)=b$ ?

THEOREM SUBSETSUM is NP-complete.

Reduction from IndSet.

Given: Undirected graph $G=(V, E)$ and positive integer $k$.

Require: finite set $X$, positive integer 'size' $s(x)$ for each $x \in X$, and integer 'goal' $b$ s.t.
$G$ has an independent set of size $k$ $\Longleftrightarrow$ there is subset $A \subseteq X$ s.t. $\sum_{x \in A} s(x)=b$.

Formally: Let
$\left\{v_{0}, \ldots, v_{n-1}\right\}:$ vertex set $V$ of $G$, $\left\{e_{0}, \ldots, e_{m-1}\right\}$ : edge set $E$ of $G$.

## Define

$$
\begin{aligned}
X & =V \cup E, \\
s\left(e_{i}\right) & =10^{i}, \quad \text { for } 0 \leq i \leq m-1 ; \\
s\left(v_{i}\right) & =10^{m}+\sum_{e_{j} \ni v_{i}} 10^{j}, \quad \text { for } 0 \leq i \leq n-1, \\
b & =k \times 10^{m}+10^{m-1}+10^{m-2}+\cdots+10^{2} \\
& +10+1 .
\end{aligned}
$$

THEOREM If $P \neq N P$ then there are languages in NP that are not in $P$ and are not NP-complete.

GRAPH ISOMORPHISM
Instance: Two undirected graphs $G=(V, E)$ and $G^{\prime}=\left(V^{\prime}, E^{\prime}\right)$.
QUESTION: Are the graphs isomorphic?

Know: GRAPH ISOMORPHISM is in NP (obvious).

Don't Know: If it is NP-complete or in P.

Curious fact: Have very few natural problems of such unknown status (hence possibly in NP but not in P.)

