Despite Ladner’s Theorem, there are very few natural problems that are:

- Known to be in NP, and
- Not known to be NP-complete, and
- Not known to be in P

**Examples:**

- Factoring natural numbers
- Graph Isomorphism
- Model Checking the $\mu$-Calculus

**Prop:** $\text{PRIME} \in \text{NP}$

**Proof:**

$$m \in \text{PRIME} \iff m < 2 \lor \exists xy \left(1 < x < m \land x \cdot y = m\right)$$

**Question:** Is $\text{PRIME} \in \text{NP}$?

**Fact 15.1 (Fermat’s Little Thm)** Let $p$ be prime and $0 < a < p$, then, $a^{p-1} \equiv 1 \pmod{p}$.

$$\mathbb{Z}_n^* = \left\{ a \in \{1, 2, \ldots, n-1\} \mid \gcd(a, n) = 1 \right\}$$

$\mathbb{Z}_n^*$ is the multiplicative group of integers mod $n$ that are relatively prime to $n$.

**Euler’s phi function:** $\varphi(n) = |\mathbb{Z}_n^*|$
Prop: If \( n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \) is the prime factorization of \( n \), then
\[
\varphi(n) = n(p_1 - 1)(p_2 - 1) \cdots (p_k - 1)/(p_1 p_2 \cdots p_k)
\]

Euler’s Thm: For any \( n \) and any \( a \in \mathbb{Z}_n^* \), \( a^\varphi(n) \equiv 1 (\text{mod } n) \).

Fact: Let \( p > 2 \) be prime. Then \( \mathbb{Z}_p^* \) is a cyclic group of order \( p - 1 \). That is,
\[
\mathbb{Z}_p^* = \{ a, a^2, a^3, \ldots, a^{p-1} \}
\]

\( m \in \text{PRIME} \iff \exists a \in \mathbb{Z}_m^* (\text{ord}(a) = m - 1) \)

Pratt’s Thm: \( \text{PRIME} \in \text{NP} \).

Proof: Given \( m \),

1. Guess \( a, 1 < a < m \)
2. Check \( a^{m-1} \equiv 1 \pmod{m} \) by repeated squaring.
3. Guess prime factorization: \( m - 1 = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \)
4. Check for \( 1 \leq i \leq k \), \( a^{m-1/p_i} \not\equiv 1 (\text{mod } m) \)
5. Recursively check that \( p_1, p_2, \ldots, p_k \) are prime.

Divide and Conquer NP Algorithm:

\[
T(n) = O(n^2) + T(n - 1)
\]

\[
T(n) = O(n^3)
\]

Cor: \( \text{PRIME} \) and \( \text{FACTORING} \) are in \( \text{NP} \cap \text{co-NP} \).

Proof: \( \text{PRIME} \): immediately from Pratt’s Thm.

\( \text{FACTORING} \) is the problem of given \( N \), find it’s prime factorization: \( N = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \).

Think of this as a decision problem by putting the factorization in a standard form, e.g., \( p_1 < p_2 < \cdots < p_k \), and asking if bit \( i \) of the factorization is “1”.

This is in \( \text{NP} \cap \text{co-NP} \) because an NP or co-NP machine can guess the unique prime factorization, check that it is correct, and then read bit \( i \).
More Primality Testing

\( a \in \mathbb{Z}_m^* \) is a **quadratic residue** mod \( m \) iff, \( \exists b \ (b^2 \equiv a \ (\text{mod } m)) \)

For \( p \) prime let,

\[
\left( \frac{a}{p} \right) = \begin{cases} 
1 & \text{if } a \text{ is a quadratic residue mod } p \\
-1 & \text{otherwise}
\end{cases}
\]

Generalize to \( \left( \frac{a}{m} \right) \) when \( m \) is not prime,

\[
\left( \frac{a}{mn} \right) = \left( \frac{a}{m} \right) \left( \frac{a}{n} \right)
\]

\[
\left( \frac{a}{m} \right) = \left( \frac{a \% m}{m} \right)
\]

**Quadratic Reciprocity Thm:** [Gauss] For odd \( a, m, \)

\[
\left( \frac{a}{m} \right) = \begin{cases} 
\left( \frac{m}{a} \right) & \text{if } a \equiv 1 \ (\text{mod } 4) \text{ or } m \equiv 1 \ (\text{mod } 4) \\
- \left( \frac{m}{a} \right) & \text{if } a \equiv 3 \ (\text{mod } 4) \text{ and } m \equiv 3 \ (\text{mod } 4)
\end{cases}
\]

\[
\left( \frac{2}{m} \right) = \begin{cases} 
1 & \text{if } m \equiv 1 \ (\text{mod } 8) \text{ or } m \equiv 7 \ (\text{mod } 8) \\
-1 & \text{if } m \equiv 3 \ (\text{mod } 8) \text{ or } m \equiv 5 \ (\text{mod } 8)
\end{cases}
\]

Thus, we can calculate \( \left( \frac{a}{m} \right) \) efficiently. For example,

\[
\left( \frac{107}{351} \right) = - \left( \frac{351}{107} \right) = - \left( \frac{30}{107} \right)
\]
\[
= - \left( \frac{2}{107} \right) \left( \frac{15}{107} \right) = - \left( \frac{107}{15} \right)
\]
\[
= - \left( \frac{2}{15} \right) = -1
\]

\( 107 \equiv 351 \equiv 15 \equiv 3 \ (\text{mod } 4) \)

\( 107 \equiv 3 \ (\text{mod } 8); \quad 15 \equiv 7 \ (\text{mod } 8) \)
Fact:[Gauss] For $p$ prime, $a \in \mathbb{Z}_p^*$, \( \left( \frac{a}{p} \right) \equiv a^{p-1} \pmod{p} \).

Fact: If $m$ not prime then,

\[
\left| \left\{ a \in \mathbb{Z}_m^* \mid \left( \frac{a}{m} \right) \equiv a^{\frac{m-1}{2}} \pmod{m} \right\} \right| < \frac{m-1}{2}
\]

**Solovay-Strassen Primality Algorithm:**

1. Input is odd number $m$
2. For $i := 1$ to $k$ do {
3. choose $a < m$ at random
4. if $\text{GCD}(a, m) \neq 1$ return (“not prime”)
5. if \( \left( \frac{a}{m} \right) \neq a^{\frac{m-1}{2}} \pmod{m} \) return (“not prime”)
6. }
7. return (“probably prime”)

**Thm:**

- If $m$ is prime then Solovay-Strassen$(m)$ returns “probably prime”.
- If $m$ is not prime, then the probability that Solovay-Strassen$(m)$ returns “probably prime” is less than $1/2^k$.

**Cor:** PRIME $\in$ “Truly Feasible”

**Fact:** [Agrawal, Kayal, and Saxena, 2002] PRIME $\in$ P

**Def:** A decision problem $S$ is in BPP (Bounded Probabilistic Polynomial Time) iff there is a probabilistic, polynomial-time algorithm $A$ such that for all inputs $w$,

- if $(w \in S)$ then $\text{Prob}(A(w) = 1) \geq \frac{2}{3}$
- if $(w \notin S)$ then $\text{Prob}(A(w) = 1) \leq \frac{1}{3}$
Prop: If $S \in \text{BPP}$ then there is a probabilistic, polynomial-time algorithm $A'$ such that for all $n$ and all inputs $w$ of length $n$,

\[
\begin{align*}
\text{if } (w \in S) \text{ then } \text{Prob}(A'(w) = 1) &\geq 1 - \frac{1}{2^n} \\
\text{if } (w \notin S) \text{ then } \text{Prob}(A'(w) = 1) &\leq \frac{1}{2^n}
\end{align*}
\]

Proof: Iterate $A$ polynomially many times and answer with the majority. Probability the mean is off by $\frac{1}{3}$ decreases exponentially with $n$ — Chernoff bounds.

Is BPP equal to P???

Probably, because pseudo-random number generators are good.

Is randomness ever useful?


Colonel Kelly:

Which base to inspect?

If we randomize, then our opponent cannot know what we will do.
Fact 15.2 Consider a random walk in a connected undirected graph $G$. Let $T(i)$ be the expected number of steps until we have reached all vertices, assuming we start at vertex $i$. Then, $T(i) \leq 2m(n-1)$, where $n = |V|$, $m = |E|$.

Corollary 15.3 UREACH $\in$ BPL.

Definition 15.4 A universal traversal sequence for graphs on $n$ nodes, is a sequence of instructions, $q = a_1a_2a_3\cdots a_t \in \{1,\ldots, n-1\}^*$, such that for any undirected graph on $n$ nodes, if we start at $s$ in $G$ and follow $q$, then we will visit every vertex in the connected component of $s$. □

Fact 15.5 Undirected graphs with $n$ vertices have universal traversal sequences of length $O(n^3)$.

Fact 15.6 (Reingold, 2004) UREACH $\in$ L

Proof idea: derandomization of universal traversal sequences using expander graphs. □

Corollary 15.7 Symmetric-L = L