P versus NP

P vs NP

NP-complete

A language $L \subseteq \{0,1\}^* \in NP - complete$ if

- $L \in NP$, and
- $L' \leq_P L$ for every $L' \in NP$.

QUADRATIC CONGRUENCES(QC)

- INSTANCE: Positive integers a, b and c, such that we have the prime factorization of b.
- QUESTION: Is there a positive integer x such that $Q(a, b, c, x) = true$ ($x^2 \equiv a (mod\ b)$ and $x < c$)?
- $QC \in NP - complete$.

$QC \in P$

- When $c = \infty$, then $QC \in P$.
- We can have a candidate solution $x \geq c$ in polynomial time such that $x^2 \equiv a(mod\ b)$.
- We must find another positive integer i such that $i < x$ and $Q(a, b, c, i) = true$.
- If this integer i exists, then $x^2 \equiv i^2(mod\ b)$.
- Therefore $x^2 - i^2 \equiv (x - i) * (x + i) \equiv 0(mod\ b)$.

$QC \in P$

- $(x - i) * (x + i) \equiv \big(x - (c - j)\big) * \big(x + (c - j)\big) \equiv 0(mod\ b)$ where $1 \leq j \leq (c - 1)$ since $i < c$.
- This means either $\big(x - (c - j)\big) \equiv 0(mod\ b)$ or $\big(x + (c - j)\big) \equiv 0(mod\ b)$ or both.
- Then $(x - c + j) \equiv 0(mod\ b)$ or $(x + c - j) \equiv 0(mod\ b)$ that is equivalent $(x - c) \equiv -j(mod\ b)$ or $(x + c) \equiv j(mod\ b)$.
- Consequently, there must exist two integers $k \geq 0$ and $k' \geq 0$ such that $(x - c) = b * k - j$ or $(x + c) = b * k' + j$.

$QC \in P$

- We need to find b' and b'' which are the nearest multiples of b which are greater than $(x - c)$ or lesser than $(x + c)$ respectively such that $b' - (x - c)$ or $(x + c) - b''$ are the possible minimum values of j greater than 0.
- Consequently, the calculation of j is trivial since it will be equal to $b' - (x - c) = j$ or $(x + c) - b'' = j$.
- We must guarantee in the calculation of b' and b'' that $b' \neq (x - c)$ and $b'' \neq (x + c)$.

$QC \in P$

- The calculation of b' and b'' can be done in polynomial time from the values $(x - c)$ and $(x + c)$.
- Certainly, b' can be calculated as

$$b' = b * \left(\left\lceil \frac{x - c}{b} \right\rceil + \left\lceil \frac{x - c}{b} \right\rceil\right)$$

- and b'' can be calculated as

$$b'' = b * \left(\left\lfloor \frac{x + c}{b} \right\rfloor - \left\lceil \frac{x + c}{b} \right\rceil\right)$$

- where $\lceil s \rceil$and $\lfloor s \rfloor$ are the ceiling and the floor functions of a real number s and $[s]$ is equal to 1 when s is an integer otherwise $[s]$ is equal to 0.

$QC \in P$

- In case of we cannot find this integer j such that $1 \leq j \leq (c - 1)$, then it will not exist $i < x$ when $Q(a, b, c, i) = true$.
- On the other hand, in case of this integer $1 \leq j \leq (c - 1)$ is found, then it will exist $c - j = i < x$ such that $Q(a, b, c, i) = true$.
- Then, $QC \in P$.

$P = NP$

- If any single $NP - complete$ problem can be solved in polynomial time, then $P = NP$.
- Since $QC \in P$ and $QC \in NP - complete$, then the answer of the P versus NP problem will be $P = NP$.
- This will break most existing cryptosystems including: public-key cryptography.
- This implies efficient solutions to many problems in operations research such as some types of integer programming and the traveling salesman.
- This could solve not merely one Millennium Problem but all seven of them assuming that the other six Clay conjectures have proofs that are not too large.

The End

- Questions?