**二、[PRIMES is in P] 出题人：曹永知**

1. 请说明文章标题“PRIMES is in P”中的“PRIMES”指什么？ （3分）

PRIMES is the decisional problem of determining whether or not a given integer is prime.

1. 文章摘要：“We present an unconditional deterministic polynomial-time algorithm determines whether an input number is prime or composite.” 请分别、简单解释 “unconditional”，“deterministic”，“polynomial-time” 这三个词在此处的含义。（6分）

“unconditional”指AKS算法不依赖/于一些未证的假设；

“deterministic”指对于同一个输入，AKS算法总是返回确定的输出（素数或者合数），不像其他随机算法有时输出素数有时输出合数；

“polynomial-time”是算法时间复杂度是输入数的位数的多项式函数。

**（意思相近即可）**

1. 给定及假设

证明： （3分）

证：由定义， 将代入，即得

/// n

1. 某同学将论文（Sec. 4）中AKS算法里的第2-4步作了如下改动（保留其他步不变）：

2. Find the smallest such that either

or

and .

3. If output PRIME.

4. If , output COMPOSITE.

请判断：修改后的算法是否具有与AKS算法同样的效果，即是否仍然是一个unconditional deterministic polynomial-time素性测试算法？（只给出判断“是”或“否”，无需说明理由。）（3分）

是。（The advantage of doing the above modifications is that it reduces the computational time involved in finding an appropriate , although the computational complexity of the whole algorithm remains unchanged.）

1. 数学家陶哲轩教授写了一篇博客文章The AKS primality test（https://terrytao.wordpress.com /2009/08/11/the-aks-primality-test/）解释AKS素性测试。下面这段话是署名Jonathan Vos Post的留言，请将其翻译成中文。 （5分）

“Thank you for the clarity in showing that PRIME is in P. Now, is SEMIPRIME in P? By definition, a semiprime is a product of exactly two primes, not necessarily distinct. They matter because of an important class of cryptosystems, in a multibillion dollar industry. The complication: there exist specific semiprimes in the literature that have been proven to be semiprimes, without any prime factorization know. We don’t know the complexity class for prime factorization. So what is the complexity class for determining if a given integer is or is not a semiprime? Several experts in number theory and quantum computing have told me that mine is an interesting question, but probably very difficult. I mention quantum computing because SEMIPRIME might be in a qc complexity class of interest. What do you think?”

谢谢你清楚地阐明判定问题PRIME属于P。现在，请问判定问题SEMIPRIME属于P吗？ 根据定义，一个半素数是两个素数的乘积，这两个素数允许相同。在一个数十亿美元的产业中，他们因为一类重要的密码系统而关系重大。困惑在于：在文献中存在特定的半素数，他们已被证明是半素数，但不知道他们的任何素因子分解。我们不知道素因子分解的复杂性类。那么判定一个给定的整数是否为半素数的复杂性类是什么呢？数论和量子计算方面的几位专家告诉我，我的问题很有趣，但可能非常困难。我提到量子计算是因为SEMIPRIME可能属于某个qc复杂性类。你怎么看？

（以上纯属意译，仅供参考。欢迎批评指正，谢谢！）