素数判定问题研究取得进展

2015-10-31 | 编辑：文\信息技术部

素数判定问题是计算数论的核心问题之一，在数论应用的各个场合都需要它，特别在密码学领域素数判定问题有重要应用。我们在素数判定问题最近有一系列的工作，包括：给出了以前9、10、11个素数为基的最小强伪素数的精确值，证明了张振祥教授的猜想；给出了广义Fermat数、形如Ap^n+w_n的特殊数的素数判定的二次确定性多项式时间算法。

素数判定是计算数论的重要问题，一直就受到数学家和计算机科学家的注意和研究。早期Gauss、Fermat等人就研究过它。在著名的公钥密码体制RSA中就使用了大素数。为了确保这些数的确是素数，就需要使用素数判定算法。故素数判定方法对于RSA 公钥密码的安全性有重要的影响。目前素数判定方法有确定性算法以及概率性算法。确定性算法由于其计算量过大而不实用。在概率性算法中，比较简单实用而快速的是著名的Miller-Rabin 算法。它基于强伪素数的性质。如果我们知道以前几个素数为基的最小强伪素数的精确值，则判定小于这个精确值的数是否为素数的方法可以由概率性算法变为确定性算法，因为只需要用前几个素数作基，看它是否通过了Miller-Rabin判别法。通过前8个素数为基的最小强伪素数的精确值早在1993年便已经知道。当时Jaeschke 还给出了以前9、10、11 个素数为基的强伪素数的上界。而后张振祥几次改进了上界并最后猜测了这些强伪素数的精确值。我们证明了张振祥的猜测，即给出了通过前9、10、11 个素数为基的最小强伪素数的精确值。论文发表在计算数学杂志《Mathematics of Computation 》上。

素数判定问题在2004年被三个印度学者Agrawal- Kayal- Saxena证明是P问题，但他们给出的AKS算法由于复杂性太高仅具理论意义而没有实际价值。另一方面，存在二次时间复杂性的素数判定的概率算法。是否存在对于一般数的二次时间复杂性的素数判定的确定性算法？这个问题如果有一个肯定的答案，那么素数判定这个问题才画上了一个完满的句号。所以说，素数判定问题还没有彻底终结，还没有死！事实上，对于特殊数存在二次时间复杂性的确定性的素数判定方法，这方面经典的例子有对于Mersenne素数的Lucas-Lehmer判别法和对于Fermat素数的Pépin判别法。我们在特殊数的更快速的素数判定方面有一些工作，即我们给出了广义Fermat数、形如Ap^n+w_n的特殊数的素数判定的二次确定性多项式时间算法，其中使用了代数数论中的高次互反律。这些工作发表在数论或算法专门杂志《Acta Arithmetica》与《Journal of Discrete Algorithms》上。