算法基础 2023 春 Homework 6

任课老师：陈雪 & 邵帅 due: June 28, 23:59

作业要求：说明思路与符号，清晰简洁的伪代码，必要的时间复杂度分析和必要的正确性分析。可以直接调用基本的数据库和已讨论过的算法/程序（如排序、找中位数、二分查找等）。

问题 1 (20 分)**.** 证明欧拉定理，即对于任意正整数 a, n 满足 $\gcd(a, n) = 1$, 有 $a^{\phi}(n) \equiv 1 \mod n$，其中 $\phi(n)$ 是欧拉函数。

问题 2 (30 分)**.** 设 (e, n) 与 (d, n) 为一对 RSA 公钥与私钥。张三将密文 P 加密为明文 $C = P^e \mod n$，准备发送给李四。过程中，王五截获明文 C，将其伪造为 $S = Cr^e \mod n$，并发送给李四。李四尝试通过私钥解密该信息，得到 $P' = S^d \mod n$。李四认为 P' 是垃圾信息并丢弃，被王五得到。

1. 为什么李四会认为 P' 是垃圾信息?
2. 王五能不能通过已知信息破译 P?
3. 为使王五能破译成功，r 需要如何选取?

问题 3 (20 分)**.** 给定一个无向图 G 和正整数 k，判断 G 中是否存在一条长度至少为 k 的简单路径 (经过每个顶点至多一次)。证明该问题是 NP 完全的。

问题 4 (20 分)**.** 已知问题 A 和问题 B 可互相多项式时间内 Karp 归约，若 A 是 NP 完全的，能否得出结论 B 也是 NP 完全的? 若是请给出证明，若否请给出反例。

问题 5 (20 分)**.** 给定一个无向图 $G = (V, E)$ 和正整数 k，G 的一个 k-因子是 G 的一个子图 H，满足对于任意 $v \in V$, v 出现在 H 中且 v 的度数为 k。(1-因子即为图的完美匹配)

给出判断一个图是否存在一个 k-因子的多项式时间算法。