# 题目 1

单　　位：西安电子科技大学

网络与信息安全学院

# Fermat 小定理

**给定素数 $p$，$a \in Z$，则有 $a^{p-1} \equiv 1\ (mod\ p)$。**

**问题1**

如果有一个整数$a$，$(a,m)=1$，使得

$$a^{m-1} \not\equiv 1(mod\ m)$$

则 $m$ 一定是一个合数。

$m=63$，　$(8,63)=1$，　$8^2 \equiv 1(mod\ 63)$

$$8^{63-1} \equiv 8^{62} \equiv \left(8^2\right)^{31} \equiv 1(mod\ 63)$$

**问题2**

如果有一个整数$a$，$(a,m)=1$，使得

$$a^{m-1} \equiv 1(mod\ m)$$

则 $m$ 一定是一个素数吗？<u>素数或伪素数</u>

以$a$为底伪素数

奇整数$m$，若任取一整数 $2 \le a \le m-2$，$(a,m)=1$，使得 $a^{m-1} \equiv 1 (mod\ m)$，则 $m$ 至少有 $\frac{1}{2}$ 的概率为素数。

# Fermat素性检验算法

奇整数 $m$，若任取一整数 $2 \le a \le m-2$，$(a,m)=1$，使得 $a^{m-1} \equiv 1 (mod\ m)$，则 $m$ 至少有 $\frac{1}{2}$ 的概率为素数。

给定奇整数 $m \ge 3$ 和安全参数 $k$

（1） 随机选取整数$a$，$2 \le a \le m-2$

（2） 计算$g=(a,m)$，如果 $g=1$，转（3）；否则，跳出， $m$ 为合数

（3） 计算 $r=a^{m-1}(mod\, m)$，如果 $r=1$，$m$ 可能是素数，转（1）；否则，跳出， $m$ 为合数

（4） 重复上述过程 $k$ 次，如果每次得到 $m$ 可能为素数，则 $m$ 为素数的概率为 $1-\frac{1}{2^k}$ 。

① 随机选取整数 $a$

② “合数”结论确定无疑，而“素数”以概率确定

概率算法

# 判定$m=277$是否为素数，并指出其可能性的概率。

解　　安全参数 $k=4$　，其可能性的概率为 $1-\frac{1}{2^4}=93.75\%$。

$a=2$，$(2,277)=1$，$2^{277-1}(mod\,277)\equiv 1$，故 $m=277$可能为素数；　　50%

$a=3$，$(3,277)=1$，$3^{277-1}(mod\,277)\equiv 1$，故 $m=277$可能为素数；　　75%

$a=5$，$(5,277)=1$，$5^{277-1}(mod\,277)\equiv 1$，故 $m=277$可能为素数；　　87.5%

$a=6$，$(6,277)=1$，$6^{277-1}(mod\,277)\equiv 1$，故 $m=277$可能为素数；　　93.75%

所以，以 $93.75\%$ 的可能性 $m=277$ 可能为素数。

奇整数 $m$，若任取一整数 $2\le a\le m-2$，$(a,m)=1$，使得 $a^{m-1}\equiv 1(mod\ m)$，则 $m$ 至少有 $\frac{1}{2}$ 的概率为素数。

# The End