费马小定理与素数测试

定理 1（Euler-Fermat）： 对互素的正整数 a, n，有 $a^{\varphi(n)} \equiv 1(mod\ n)$

证明： 称与 n 互素且不大于 n 的所有数为 $mod\ n$ 的**缩系**.

考虑 $n = 16, a = 3$.

$S = \{1, 3, 5, 7, 9, 11, 13, 15\}$ 为 $mod\ 16$ 的缩系，故 $\varphi(n) = |S| = 8$

在 mod 16 的意义下将缩系中每个元素扩大三倍,可以得到 $S' = \{3, 9, 15, 5, 11, 1, 7, 13\} = S$.

$$\begin{aligned} 1 \times 3 \times 5 \times \cdots \times 15 &\equiv 3 \times 9 \times 15 \times \cdots \times 13 \\ &\equiv 3^8 \times 1 \times 3 \times 5 \times \cdots \times 15(mod\ 16) \end{aligned}$$

$\therefore 3^8 \equiv 1(mod\ 16)$

也可利用环来证明.

推论（费马小定理）： 若 p 为素数，则 $a^p \equiv a(mod\ p)$.

费马素数测试

对一个足够大的奇数，取 $a = 2$，若 $2^n \not\equiv 2(mod\ n)$，则 n 为合数

$2^n \equiv 2(mod\ n)$，则 n 通过了底为 2 的费马素数测试

定义： 若一个合数 n 也通过了底为 a 的费马素数测试，则称其为底为 a 的**费马伪素数**.

若合数 n 通过了所有底的费马素数测试，则称 n 为 **Carmichael 数**.

Q: 有 Carmichael 数存在吗？若有，是无穷多个吗？

A: Carmichael 数存在且有无穷多个.

底为 a 的 Miller 素数测试

设 n 为一较大的奇数，令 $n - 1 = 2^r s, r \geq 1, s$ 为奇数

验证一下 $r + 1$ 个同余式是否成立：

$$a^s \equiv 1(mod\ n)$$

$$
\begin{gathered}
a^s \equiv -1(mod\ n) \\
a^{2s} \equiv -1(mod\ n) \\
\vdots \\
a^{2^{r-1}s} \equiv -1(mod\ n)
\end{gathered}
$$

若至少一个成立，则称 n 通过了 Miller 测试

例：$n = 341$ 是底为 2 的伪素数.

$$
\begin{gathered}
n - 1 = 340 = 2^2 \times 85, r = 2, s = 85 \\
2^{85} \not\equiv 1(mod\ 341) \\
2^{85} \not\equiv -1(mod\ 341) \\
2^{2^{85}} \equiv -1(mod\ 341)
\end{gathered}
$$

故 341 未通过底为 2 的 Miller 测试

求证：所有素数 p 均可通过底为 a 的 Miller 素数测试 $(p \neq a)$

证明：由费马小定理，$a^{p-1} \equiv 1(mod\ p), p - 1 = 2^r s$

则 $a^{\frac{p-1}{2}} \equiv 1(mod\ p)$ 或 $a^{\frac{p-1}{2}} \equiv -1(mod\ p)$

由第一个式子 $a^{\frac{p-1}{4}} \equiv 1(mod\ p)$ 或 $a^{\frac{p-1}{4}} \equiv -1(mod\ p)$

$\vdots$

$a^s \equiv 1(mod\ p)$ 或 $a^s \equiv -1(mod\ p)$

定义：若 n 为合数且通过了底为 a 的 Miller 素数测试，则称 n 为底为 a 的**强伪素数**.

注记：Miller 素数测试强于费马素数测试，故所有的强伪素数也是伪素数（底为 a）

定理 2：设 n 为较大正整数，对所有底 $1 \leq a \leq n-1$，数 n 至多通过 $\frac{n-1}{4}$ 个底的 Miller 测试.

注记：若 n 通过了许多底的 Miller 测试，则 a 极有可能为一素数.