数学之美--读后感

勾股定理（毕达哥拉斯定理）

$$x^2 + y^2 = z^2$$

费马大定理

$$x^n + y^n \neq z^n (x, y, n \in \mathbb{N}1, n \geq 3)$$

费马大定理由17世纪法国数学家皮耶·德·费玛提出，历经三百多年的历史，最终在1995年被英国数学家安德鲁·怀尔斯彻底证明。

黎曼猜想

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} (Re(s) > 1, n \in \mathbb{N}1)$$

ζ 函数的所有非平凡零点都位于复平面上 Re(s)=1/2 的直线上，也即方程ζ(s)=0的解的实部都是1/2,至今未被证明。黎曼猜想是关于素数分布的问题，素数也就是质数。

RSA加密与解密

加密函数 $m^e \equiv c \pmod n$
解密函数 $c^d \equiv m \pmod n$

原理

1. 找到两个互不相等的素数p、q
2. 计算p和q的乘积n。n = p * q
3. 计算n的欧拉函数$\phi(n)$：

$$\phi(n) = (p-1) * (q-1)$$

4. 随机选取一个整数e，e与$\phi(n)$互质，并且e满足如下条件：

$$1 < e < \phi(n)$$

5. 计算e对于$\phi(n)$的模反元素d($d \in \mathbb{Z}$)：

$$e * d \equiv 1 \pmod{\phi(n)}$$

根据上面五个步骤，我们得到了p、q、n、e、d、$\phi(n)$。其中（n，e）为公钥、（n，d）为私钥

安全性--破解私钥(n,d)

> "对极大整数做因数分解的难度决定了RSA算法的可靠性。换言之，对一极大整数做因数分解愈困难，RSA算法愈可靠。
>
> 假如有人找到一种快速因数分解的算法，那么RSA的可靠性就会极度下降。但找到这样的算法的可能性是非常小的。今天只有短的RSA密钥才可能被暴力破解。到2008年为止，世界上还没有任何可靠的攻击RSA算法的方式。
>
> 只要密钥长度足够长，用RSA加密的信息实际上是不能被解破的。"