快速幂与慢速乘

Ⅰ. 快速幂：

一. 用途：在 log(n)的时间内，求得 a^n 的值[1]

二. 引理：任意一个正整数都可以写成 2 的整次方幂相加的形式

证明：可以使用数学归纳法证明。不过最简单、最直接的方法还是类比 10 进制整数在二进制下的表示：每 n 位的 1 or 0 对应 2^{n-1} 取或不取。

三. 算法实现：

不妨设，我们要求 a^n：

由引理可得，n 可被拆成至多 log(n)个不同的 2 的整次方幂。

所以我们只需要求得 $a^{1\sim\lfloor\log_2(n)\rfloor}$ 即可。

四. 代码参考：http://paste.ubuntu.com/17970611/[2]

五. 矩阵快速幂：原理与快速幂完全一样[3]，所以只需要重载“*”即可

Ⅱ. 慢速乘：

一. 用途：在 log(b)的时间内完成计算 a*b[4]

二. 引理：+、−、*这三个基本运算中可以随时取模[5]

三. 算法实现：

将 b 进行二进制拆分[6]，分别与 a 相乘，相乘后马上取模

四. 代码实现：http://paste.ubuntu.com/17971967/（二进制拆分版本）

http://paste.ubuntu.com/17972151/（十进制拆分版本）

---

[1] 题目一般会在 Mod P 的意义下求取此值以避免乘法溢出

[2] 板题参考：http://oi.cdshishi.net:8080/Problem/25

[3] 因为矩阵乘法也满足交换律与结合律

[4] 一般适用于 a，b 较大，直接相乘会使 long long 溢出的情况，题目参考 http://www.lydsy.com

[5] 这个说法极不严谨，但却十分易懂

[6] 同上文提到的“拆成 2 的整次方幂”，也可进行在 10 进制下直接拆解