逆元

Ⅰ. 引入：

我们知道，对于+，-，*这三个基本运算，可以直接 Mod P，但 / 不行[1]。

但如果我们规定 X^{-1} 满足 $X * X^{-1} \equiv 1 \pmod{P}$，那么我们想在 Mod P 的意义下，除以 X^2，就可以用乘以 X^{-1} 来代替[3]

Ⅱ. 相关定理：

m 的简约剩余系 Z*中的余数 a[4]，总存在 b∈Z*，使得 ab≡1(Mod m)，即同 余方程 ax≡1(mod)总是有唯一解。

Ⅲ. 单个逆元的求解

由“$X * X^{-1} \equiv 1 \pmod{P}$”形式，不难想到拓展欧几里得算法。

故单个数的逆元，可以用拓展欧几里得算法[5]求解[6]。

题目参考：http://oi.cdshishi.net:8080/Problem/256

代码参考：http://paste.ubuntu.com/17910887/

Ⅳ. 批量处理逆元

假如我们需要处理 1～(P-1) 在 Mod P 的意义下的逆元，则我们可以采用递推的形式求解。

---

[1] 由不完全归纳法可以得出上述结论，详细证明还有待探究
[2] 这么直接做是不行的，可以自己出几个数试一试
[3] 这样做是可以的，见脚注 1
[4] 即 a，m 互质
[5] 可参见本博客：【算法笔记】欧几里得算法（GCD）与拓展欧几里得算法（EXGCD）·基础
[6] 因为需要用到 GCD（Mod, x）= 1，所以必须满足脚注 4

推导如下：

假设我们已经处理出了 1~(i-1)所有存在的逆元(Mod P)，现在来处理 i[7]。

设 $P = k * i + r$

则 $i = (P-r) / k \quad => \quad i \equiv -r / k \ (Mod\ P)$

所以 $-r / k * i^{-1} \equiv 1 \ (Mod\ P)$

所以 $i^{-1} \equiv -k * r^{-1} \ (Mod\ P)$

即 $i^{-1} = -k * r^{-1} \quad => \quad i^{-1} = -(P / i) * (P \% i)^{-1}$

所以 $i^{-1} = (P-(P / i))^{8} * (P \% i)^{-1}$

代码参考：http://paste.ubuntu.com/17912971/[9]

Ⅴ. 其他求解逆元的方法[10]

因为其他方法不常用[11]，故留下一神犇的博客，有兴趣者可以自行研究：

http://syncshinee.github.io

---

[7] 不妨设 i 与 P 互质

[8] 保证其为正数

[9] 非本人代码

[10] 不同的求解逆元的方法有不同的局限性，要特别注意选择

[11] 其中使用费马小定理的方法个人认为十分优美，只需要一个快速幂即可。但因为要求 P 必须是质数，局限性太大，故不展开讨论