求解x=a^b(mod m)

Posted on 2012 年 11 月 6 日 by NARUTOACM —

本文致力于解决如下问题：**求解$x \equiv a^b$(mod m)，其中a,b,m都是正整数。**

如果b足够小，则可直接用**逐次平方法**求解，如果你不知道逐次平方法，可以先看这里。所以这里假设b足够大（这不是说是一个64位整数，而是可以上百上千位的一个数），大到逐次平方法也已不足以快速出解。

用素数探路的思想，先假设m是素数，那么要么a与m互素，要么m|a。前者可利用**费马小定理**，令b = k(m-1) + b′，其中0≤b′<m-1，则有$a^b \equiv a^{k(m-1)+b'} \equiv a^{b'}$(mod m)。之后可用逐次平方法快速求解。若m|a，结果显然为0。

现在考虑要求m可以是任意数的情况。同样，若a与m互素，由上边我们可联想到**欧拉公式**，利用欧拉公式求解。令b = kΦ(m) + b′，其中0≤b′<Φ(m)，则有$a^b \equiv a^{k\Phi(m)+b'} \equiv a^{b'}$(mod m)，之后用逐次平方法快速求解。如果a与m不互素，即gcd(a,m)>1，这种情况下应该怎么做？

注意到b如此大，而模m的不同的数最多只有m个，显而易见的，**a^b一定和某个很小的指数$a^{b'}$模m同余**，如果找到这个小的指数，就可以利用逐次平方法求解。考虑如下序列：

$$a^0, a^1, ..., a^m(\text{mod } m)$$

由鸽巢原理可知，必有一个**最小的r和一个最小的s**，使得$a^r \equiv a^{r+s}$(mod m)，其中r+s≤m。若找到这样的r和s，那么显然有$a^x \equiv a^{kr+x0} \equiv a^{kr+s+x0} \equiv a^{x+s}$(mod m)，其中x是大于或等于r的任意数。要注意的是，**对任意大于或等于r的x，不存在更小的数s1，使得$a^x \equiv a^{x+s1}$(mod m)**。假如有更小的这样的数s1存在，不妨设x = r+ks，因为若不这样，可以令x1 = x + x′ = r + ks，同余式两边同时乘以$a^{x'}$，就变成$a^{x1} \equiv a^{x1+s1}$(mod m)，而x1 = r+ks。所以有$a^x \equiv a^{r+ks} \equiv a^r \equiv a^{r+s1}$(mod m)，其中s1<s，这与我们找到的s是最小的相矛盾，所以这样的s1是不存在的。上面的论述给出以下的一个事实：序列

$$a^0, a^1, ..., a^k, ...(\text{mod } m)$$

实际上是这样一个序列

$$a^0, a^1, \ldots, a^r, a^{r+1}, \ldots, a^{r+s-1}, a^r, a^{r+1}, \ldots (\mathrm{mod}\ m)$$

即**a的0次、1次...幂模m的序列中，前r个数互不相同，从第r+1个数(注：指数为r)开始，每s个数就循环一次**。我们把**r称为a幂次模m的循环起始点，s称为循环长度**。根据以上推导，如果我们能够找到r和s，那么大幂次b就能转换成一个小于m的幂次，然后用逐次平方法就可以求出问题的解。

不妨把a分解成素数乘积的形式：$a = p_1^{a1}p_2^{a2}\ldots p_n^{an}$，那么a的b次幂模m就转换成每个素数的若干次幂模m的结果相乘再模m，而素数和m的关系只有两种，一种是互素，另一种是m的约数。第一种情况我们已经解决了，所以现在的问题转换成求素数p的b次幂模m，即$p^b(\mathrm{mod}\ m)$，其中p|m。

如前所述，我们可以找到幂模m的r和s，使得$p^r \equiv p^{r+s}(\mathrm{mod}\ m)$。于是$m|(p^{r+s} - p^r)$，即$m|p^r(p^s - 1)$，令$m = p^{r0}m'$，其中gcd(p,m′)=1。因为$gcd(p,p^s - 1)=1$，所以r至少为r0，即r≥r0，由r的最小性可得**r即为r0**。于是有$m'|(p^s - 1)$，即有$p^s \equiv 1(\mathrm{mod}\ m')$。由s的最小性可知，我们只需要找出**最小的一个使上式成立的指数，该指数即为s**。事实上，这个指数叫做**p模m′的次数**。

次数定义：对任意正整数a与m，其中gcd(a,m)=1，使得$a^e \equiv 1(\mathrm{mod}\ m)$的最小指数e≥1叫做a模m的次数，记作$e_m(a)$。

现在证明如下次数性质：**若有$a^n \equiv 1(\mathrm{mod}\ m)$，则次数$e_m(a)$整除n。特别的，次数总整除Φ(m)**。

证明：令$g = gcd(n,e_m(a))$，则求得x, y使得$nx + e_m(a)y = g$，于是有$a^{nx} \equiv 1 \equiv a^g(\mathrm{mod}\ m)$，由次数的最小性可得$g = e_m(a)$，即有$e_m(a)|n$。又欧拉公式告诉我们$a^{\Phi(m)} \equiv 1(\mathrm{mod}\ m)$，结合上边推理可知次数总整除Φ(m)。证毕！

由次数定义极其性质可知，**s即为$e_{m'}(p)$，并且s|Φ(m′)**。由于$m = p^{r0}m'$，且gcd(p,m′)=1，由欧拉Φ函数的积性可得Φ(m′)|Φ(m)，这说明**s|Φ(m)**。所以有$p^x \equiv p^{x+\Phi(m)}(\mathrm{mod}\ m)$, x≥r=r0，于是$p^b \equiv p^{r+(b-r)(\mathrm{mod}\ \Phi(m))}(\mathrm{mod}\ m)$。由于$m = p^r m'$，所以$\Phi(m) \geq \Phi(p^r) = p^{r-1}(p-1) \geq r$，其中最后一步可用数学归纳法证明。所以

$$\mathbf{p^b \equiv p^{r(\mathrm{mod}\ \Phi(m))+\Phi(m)+(b-r)(\mathrm{mod}\ \Phi(m))} \equiv p^{\Phi(m)+b(\mathrm{mod}\ \Phi(m))}(\mathrm{mod}\ m)}$$

现在我们可以把a分解成素数乘积，然后对于乘积中每个素数，求出对应幂次模m的值，然后相乘再模m，就得出了解！

能否直接求出a的幂次模m的循环起始点r和循环长度s？！

假设素数p的幂次模m的循环起始点r0和循环长度s0已经求出了，那么**p^a的幂次模m的循环起始点和循环长度是多少？**同样的分析方法，设循环起始点为r，循环长度为s，则有m|p^{ra}(p^{sa} - 1)，根据前面的论述，我们知道m = p^{r0}m′，其中gcd(p,m′)=1，所以ra≥r0 → r≥r0/a → r≥ceil(r0/a)，**由r的定义的最小性可得r = ceil(r0/a)**。同样又有m′|(p^{sa} - 1)，即p^{sa}≡1(mod m′)，**所以s = $^{s0}/_{gcd(s0,a)}$，即有s|s0|Φ(m)**。

设数a0的幂次模m的循环起始点为r0，循环长度为s0，数a1的幂次模m的循环起始点为r1，循环长度为s1，其中gcd(a0,a1)=1。现在，**我们求a0a1的幂次模m的循环起始点r和循环长度s**。由已知可得m|$a0^{r0}$($a0^{s0}$ - 1)，又显然gcd(a0,$a0^{s0}$-1)=1，因为r0是循环起始点，所以m = $a0^{r0}$m′，其中gcd(a0,m′)=1。同理也有m = $a1^{r1}$m″，其中gcd(a1,m″)=1。又由于gcd(a0,a1)=1，所以有m = $a0^{r0}a1^{r1}$n，其中gcd(a0,n)=gcd(a1,n)=1。由m|$(a0a1)^r((a0a1)^s$-1)且gcd(a0a1,$(a0a1)^s$-1)=1且gcd(a0,a1)=1可得，r≥r0且r≥r1。**由r的最小性知r即为max(r0,r1)**。于是n|($(a0a1)^s$-1)，即$(a0a1)^s$≡1(mod n)，**所以s = e_n(a0a1)**。又m′|($a0^{s0}$-1)，而n|m′，所以$a0^{s0}$≡1(mod n)。同理有$a1^{s1}$≡1(mod n)。所以$(a0a1)^{lcm(s0,s1)}$≡$a0^{lcm(s0,s1)}a1^{lcm(s0,s1)}$≡1(mod n)，**由次数性质可得s|lcm(s0,s1)**。

当把a分解成素数乘积a = $p_1^{a1}p_2^{a2}...p_n^{an}$时，以上讨论告诉我们**a的幂次模m的循环起始点r = max(ceil(ri/ai)),(1≤i≤n)，其中ri是m中包含p_i的最大次数。a的幂次模m的循环长度s|lcm($^{si}/_{gcd(si,ai)}$),(1≤i≤n) |Φ(m)，其中si为p_i的幂次模m的循环长度**。因为ri<=Φ(m)，所以r<=Φ(m)。因此有

$$a^b \equiv a^{r+(b-r)(\mathrm{mod}\ s)} \equiv a^{r+(b-r)(\mathrm{mod}\ \Phi(m))} \equiv a^{b(\mathrm{mod}\ \Phi(m))+\Phi(m)} (\mathrm{mod}\ m)$$

问题解决！（所有公式都没用mathjax显示，看起来可能有点别扭~）

This entry was posted in **数论** and tagged **幂模**, **循环节**, **次数**, **欧拉公式**, **费马小定理**, **逐次平方法** by **NARUTOACM**. Bookmark the **permalink** **[http://www.narutoacm.com/archives/a-pow-b-mod-m/]** .

15 thoughts on “求解X=A^B(MOD M)”

xpc

on **2012 年 11 月 6 日 at 21:55** said:

抢大神沙发

NARUTOACM

on **2012 年 11 月 6 日 at 22:09** said:

Orz大神！

惜阳

on **2012 年 11 月 8 日 at 16:46** said:

(⊙o⊙)哇，发文章的频率这么高……

NARUTOACM

on **2012 年 11 月 8 日 at 18:07** said:

这。。超慢啊

klion26

on **2012 年 11 月 10 日 at 16:14** said:

ORZ!

NARUTOACM

on **2012 年 11 月 10 日 at 22:13** said:

Orz！！

lazycal

on **2013 年 10 月 19 日 at 21:38** said:

大神那个模的定理是您自己推导出来的吗？还有那个定理叫什么。。。网上的证明很少啊，大神的证明写的实在是太好了。我是福建的OIer，以前都叫那个定理“求幂大法”的，然后不会证，看了大神的博客，感觉有种彻悟的感觉……Orz

> 
>
> NARUTOACM
>
> on **2013 年 10 月 20 日 at 09:22** said:
>
> 我也不知道那个定理叫个什么名字，这里所有东西都是我自己推出来的，见笑= =
>
> > 
> >
> > **lazycal**
> >
> > on **2013 年 10 月 20 日 at 11:08** said:
> >
> > orz大神。
> > http://hi.baidu.com/aekdycoin/item/e493adc9a7c0870bad092fd9
> > 这里面也有个证明，是某位大神在10年写的。这个定理好像有点历史的样子…
> >
> > > 
> > >
> > > NARUTOACM
> > >
> > > on **2013 年 10 月 21 日 at 09:24** said:
> > >
> > > 那个blog是一个数论巨犇的，Orz！

Pingback: 数论同余专题总结 | WHUAtum

Pingback: (转载)数论同余专题总结 | Atum

Pingback: (转载)数论同余专题总结 | WHUAtum

Pingback: [ACM] UVaOJ 10692 Huge Mods (指数循环节) | FreeMeepo

Pingback: 第九周周赛——周赛兼组队赛第一场题解（出自HDU5443，本oj，HDU 5667，poj1742，codeforces 664A，BUNOJ 28199） - 编程语言 - 阿里欧歌