知乎 首发于 算法数学笔记

（扩展）中国剩余定理

对方正在输入 + 关注他

零、序言

第六章讲了可以处理同余方程的扩展欧几里得算法。这一章，我们将更进一步，利用中国剩余定理，处理一下同余方程组。

本文需要读者理解扩展欧几里得算法和对应不定方程组解的分布规律，如果不明白可以阅读我的前面一篇文章：

一、中国剩余定理

中国剩余定理定理是处理一类模数互质的同余方程的方法。具体地说，就是指以下这种形式的方程：

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\cdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

其中 $m_1, m_2, \cdots, m_n$ 间两两互质。

我们构造型地得出方程的解：令 $M = m_1 m_2 m...m_n$，$M_k = \dfrac{M}{m_k}$，y_k 为 M_k 在模 m_k 意义下的逆元。

注意这里的逆元是一定存在的，因为模数两两互质，可以用扩展欧几里得算法得到。

那么我们得到方程的解 $x = \sum_{i=1}^{n} a_k M_k y_k$。

原因是这样的：考虑任意一个 $i \le n$，第 i 组方程是 $x \equiv a_i \pmod{m_i}$。对于解 x 的第 i 项在模 m_i 时，$M_i y_i = 1$，于是第 i 项 $a_i M_i y_i = a_i$。

对于任意的不是第 i 组的情况，记 $j \neq i$。由于 M_j 的定义，显然 $m_i \mid M_j$。于是 $M_j \equiv 0 \pmod{m_j}$，所以说其余项均为 0。

下面我们证明解的分布情况：对任意的两个解 p, q，有 $p \equiv q \pmod{M}$。

因为 $p \equiv q \equiv a_k \pmod{m_k}$，所以说 $m_k \mid (p - q)$。

因为每一个 m_k 都整除 $p - q$，而各个 m_k 之间又没有共用因子，所以说 M 也整除 $p - q$。

因此 $p \equiv q \pmod{M}$。

不难看出，复杂度为 $O(n \log m)$，其中 m 为模数大小。

知乎 首发于 算法数学笔记

对于模数不互质的情况，我们可以通过合并相邻两组方程的方式来逐步得到解。

举个例子，我在这里面随便挑两组方程 $x \equiv a_i \pmod{m_i}$ 和 $x \equiv a_j \pmod{m_j}$。

我们把它转化成一般形式： $x + y_i m_i = a_i$ 和 $x + y_j m_j = a_j$。

移项，得到 $a_i - y_i m_i = x$ 和 $a_j - y_j m_j = x$。也就是 $a_i - y_i m_i = a_j - y_j m_j = x$。

再移项，得到 $a_i - a_j = y_i m_i - y_j m_j$。

现在， a_i, a_j, m_i, m_j 都是已知的，只有 y_i, y_j 是未知的。我们不妨把它看成是关于 y_i, y_j 的不定方程，那么根据Bézout定理，如果 $\gcd(m_i, m_j) \nmid a_i - a_j$ 的话，这组方程是无解的，从而导致整个方程组是无解的。

那如果有解怎么办呢？首先我们可以使用扩展欧几里得算法求出一组 y_i, y_j，然后带回去得到 x 的一个特解。不过现在我们的问题在于，存在无穷多组解，使得我们即使求出了其中一对方程的解也无法确定哪个是我们最终想要的。

不过好消息是，扩展中国剩余定理告诉我们，两组这样的同余方程可以在不舍去根的情况下合并成一个方程。下面是扩展中国剩余定理的核心内容：

对于方程组 $\begin{cases} x \equiv u \pmod{p} \\ x \equiv v \pmod{q} \end{cases}$ ，记特解为 x_0 ，则有通解 $x = x_0 - k\operatorname{lcm}(p, q)$ ，即这个方程组等价于方程 $x \equiv x_0 \pmod{\operatorname{lcm}(p, q)}$。

这个结论虽然看起来比较棘手，但是我们通过第六章的铺垫，推导也并不困难：

首先原方程组等价于 $\begin{cases} x + py = u \\ x + qz = v \end{cases}$ ，即 $\begin{cases} x = u - py \\ x = v - qz \end{cases}$ ，即 $u - py = v - qz$，最后化简成 $py - qz = u - v$。（这里的 y, z 都是同余方程转成不定方程的未知数）

假设我们求得了一组特解 y_0, z_0 ，根据第六章我们得到的结论，这个方程的整个解系为：

$$\begin{cases} y = y_0 + k\dfrac{q}{\gcd(p, q)} \\ z = z_0 - k\dfrac{p}{\gcd(p, q)} \end{cases}$$

我们通过 y_0 ，也可以得到 x 的一个特解 $x_0 = u - py_0$。

x 的通解为：

$$\begin{aligned} x &= u - p\left(y_0 + k\frac{q}{\gcd(p, q)}\right) \\ &= u - py_0 - k\frac{pq}{\gcd(p, q)} \\ &= x_0 - k\frac{pq}{\gcd(p, q)} \\ &= x_0 - k\operatorname{lcm}(p, q) \end{aligned}$$

于是我们证明了这个核心结论。换句话来讲，我们也得到了 $\begin{cases} x \equiv u \pmod{p} \\ x \equiv v \pmod{q} \end{cases}$ 等价于 $x \equiv x_0 \pmod{\operatorname{lcm}(p, q)}$。

于是我们就得到了扩展中国剩余定理的算法流程：

- 首先维护一个方程组列表，存储了所要求的方程组

- 然后把原来的两个方程从列表中删除。
- 最后再插入新的等价方程 $x \equiv x_0 \pmod{\operatorname{lcm}(p, q)}$。
- 如果当前剩余方程数量 ≥ 2，就继续进行第二步。
- 最后只剩下一个方程，我们可以用扩展欧几里得算法轻易地求解。

这里的顺序并不影响我们的算法流程。

以上就是关于（扩展）中国剩余定理的全部内容。

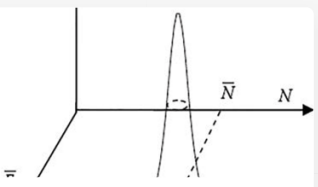
编辑于 2023-01-04 15:49 · IP 属地山东

算法 数学 数论

文章被以下专栏收录

算法数学笔记
与算法紧密相关的数学知识

推荐阅读



巨正则系综中的粒子数涨落与能量涨落
大宅学家

中国剩余定理的一个证明
冯克勤《近世代数引论》（第三版）P73中国剩余定理的证明，我看了几遍没弄懂，琢磨了半天，弄出了下面一个比较直观点的证明，写出来供参考。 【中国剩余定理】 设R是含幺环， I_{1},I_{2},.…
石劲松

中国剩余定理和大衍求一术
作为一个直接以中国命名的定理，中国剩余定理是中国古代数学在数论领域的最重要成果，也是数学主要分支的基础定理里少有被世界公认为属于中国的。值得说明的是，中国古代的数学家不仅给出了…
Sliark

知乎 首发于 算法数学笔记