非质数二次剩余

解方程 $x^{2}\equiv a\pmod{p^{n}}$这里先讨论 p 是奇质数，且 $(a,p)=1$ 的情况。

若 $x^{2}\equiv a\pmod{p}$ 无解，那么显然原方程也无解。否则设 r 是一个根，那么 $(r^{2}-a)^{n}\equiv0\pmod{p^{n}}$又由于 $(r-\sqrt{a})^{n}=t-s\sqrt{a}$$(r+\sqrt{a})^{n}=t+s\sqrt{a}$因此 $t^{2}-s^{2}a\equiv0\pmod{p^{n}}$同时可以证明$t,s$ 总是 2 的幂乘上 r,a 的多项式，因此 t,s 均与 p 互质。其中一个解为 $t^{2}\cdot s^{-2}$

注意到恰有 $\frac{(p-1)p^{n-1}}{2}$ 个余数有解，而每个余数均至少有两个不同的解，因此每个余数恰有两解。

若 $(a,p)\neq1$简单讨论 a 中有几个 p 即可。

若 $p=2$可以递归地解 $x^{2}\equiv a\pmod{p^{1},p^{2},\ldots,p^{n}}$因为 p 只有 2，所以每层也只用验证 $O(2)$ 个数，比较简单。