Solution

a

将所有二进制表示下数码1出现偶数个的非负整数归入集合S_a，其他非负整数归入另一个集合S_b，则S_a, S_b是满足条件的分划。

注意到，S_a中满足$s_1 \in S_a, s_2 \in S_a, s_1 \neq s_2,$且$s_1 + s_2 = k$（$k \leqslant n$) 的数对$(s_1, s_2)$,由于$s_1 \neq s_2$,因此在二进制表示下$s_1, s_2$必有一位不同。从右到左看，第1个不同数码的数位上，改变$s1, s2$在这一位上的数码，分别得到a_1, a_2。则有$a_1 \in S_b, a_2 \in S_b, a_1 \neq a_2,$且$a_1 + a_2 = k(k \leqslant n)$.而$(a_1, a_2)$是一个$S_b$中的数对。

两元素均在 S_a中的每一个数对，都可以通过这样的方法映射为，两元素均在 S_b中的一个数对。而两元素均在S_b中的每一个数对，也可以通过类似的方法映射为，两元素均在S_a 中的一个数对。

容易证明这样的分划是唯一的。

b

离线的多维偏序问题。

可以使用：CDQ套CDQ以及多种方法解决（树套树套树，CDQ套BIT套Treap？）

c

当m为模4余3的素数时

当p为模4余3的素数时，$X_0 = a^{(p+1)/4}$ 是方程$X^2 \equiv a(mod\, p)$ 的一个解。

证明：

当p为模4余3的素数时，$(p+1)/4$ 为整数。

如果方程有解，则由欧拉准则有：

$$a^{p-1/2} \equiv (\frac{a}{p}) \equiv 1(mod\, p)$$

$$X_0^2 \equiv (a^{(p+1)/4})^2 \equiv a^{(p+1)/2} \equiv a^{(p-1)/2+1} \equiv a^{(p-1)/2} * a \equiv a(mod\, p)$$

当m为模5余8的质数时

当p为模8余5,的素数时，$X_0 = a^{(p+3)/8}$ 或 $X_0 = 2a \times (4a)^{(p-5)/8}$ 是方程$X^2 \equiv a(modp)$的一个解。

证明：https://www.physicsforums.com/threads/where-does-p-5-mod-8-solve-x-2-a.594431/

当m为普通奇质数时

解方程：

$$x^2 \equiv a(mod\, p), p\text{为质数}$$

当$a = 0$时，$x \equiv 0(mod\, p)$.

当$a \neq 0$时，使用欧拉准则判断方程是否有解。

如果有解，令$p - 1 = 2^t \times s$，$(2 \nmid s)$

A) 当$t = 1$时，

$$\sqrt{a} = \sqrt{a^{\frac{p-1}{2}} \times a} = \sqrt{a^{s+1}} = a^{\frac{s+1}{2}}$$

B) 当$t \neq 1$时，令$x_{t-1} = a^{\frac{s+1}{2}}$

$$(a^{-1} \times (x_{t-1})^2)^{2^{t-1}} = a^{\frac{p-1}{2}} \equiv 1(mod\, p)$$

我们求的是：

$$(a^{-1} \times (x_0)^2)^{2^0} \equiv 1(mod\, p)$$

现在考虑x_{t-k}到$x_{t-(k+1)}$的递推

令$\epsilon_i = a^{-1} \times x_i^2$

有

$$\epsilon_{t-k}^{2^{t-(k+1)}} \equiv \pm 1(mod\, p)$$

a)

$$\epsilon_{t-k}^{2^{t-(k+1)}} \equiv +1(mod\, p)$$

$$\epsilon_{t-k} = \epsilon_{t-(k+1)}$$

$$x_{t-(k+1)} = x_{t-k}$$

b)

$$\epsilon_{t-k}^{2^{t-(k+1)}} \equiv -1(mod\, p)$$

试图找到一个λ使得

$$\epsilon_{t-(k+1)}^{2^{t-(k+1)}} = (a^{-1} \times (\lambda \times x_{t-k})^2)^{2^{t-(k+1)}} \equiv +1(mod\, p)$$

此时$x_{t-(k+1)}=\lambda\times x_{t-k}$

当λ满足条件时，有

$$(a^{-1}\times(x_{t-k})^2)^{2^{t-(k+1)}}\times\lambda^{2^{t-k}}\equiv+1(mod\,p)$$

$$\lambda^{2^{t-k}}\equiv-1(mod\,p)$$

假设b是模p的二次非剩余。

$$b^{2^{\frac{p-1}{2}}}\equiv b^{2^{t-1}\times s}\equiv(b^{2^{k-1}\times s})^{2^{t-k}}\equiv-1(mod\,p)$$

$$\lambda=b^{2^{k-1}\times s}$$

p恰好有$\frac{p-1}{2}$个二次非剩余，随机选取b即可。

复杂度为$O(t^2)$

最终的答案是$X_0=x_0$,方程的另一个解是$X_1=p-X_0$.

当p为普通偶质数时

即$p=2$,特判即可。