数学题选讲

唐靖哲

北京航空航天大学计算机学院

2017 年 3 月 17 日

整体内容

- 质数筛法 versus 启发式分解 March 11th, 2017
- 离散对数与原根 March 17th, 2017
- 容斥原理与二项式系数 To Be Determined
- ~~互动交流~~

离散对数与原根

- 缩系：模 m 意义下与 m 互质的元素组成缩系，缩系中任意两个元素的乘积还在缩系中，缩系的大小是 $\varphi(m)$
- 阶：满足 $x^r \equiv 1 \pmod m$ 最小正整数 r 称为 x 的阶 $\mathrm{ord}_m(x)$
- 原根：缩系中存在元素 g 使得 g^i $(i = 1, 2, \cdots, \varphi(m))$ 两两不同，则称 g 是模 m 意义下的原根，也意味着缩系中的元素可以表示成 g 的幂次，不难得到 $\mathrm{ord}_m(g) = \varphi(m)$
- 指标：若缩系有原根 g，则元素 $x \equiv g^i \pmod m$ 关于 g 指标为 $\mathrm{ind}_{m,g}(x) = i \bmod \varphi(m)$，显然 $\mathrm{ord}_m(x) = \frac{\varphi(m)}{\gcd(\varphi(m), \mathrm{ind}_{m,g}(x))}$

离散对数与原根

- 缩系：模 m 意义下与 m 互质的元素组成缩系，缩系中任意两个元素的乘积还在缩系中，缩系的大小是 $\varphi(m)$
- 阶：满足 $x^r \equiv 1 \pmod m$ 最小正整数 r 称为 x 的阶 $\mathrm{ord}_m(x)$
- 原根：缩系中存在元素 g 使得 g^i $(i = 1, 2, \cdots, \varphi(m))$ 两两不同，则称 g 是模 m 意义下的原根，也意味着缩系中的元素可以表示成 g 的幂次，不难得到 $\mathrm{ord}_m(g) = \varphi(m)$
- 指标：若缩系有原根 g ，则元素 $x \equiv g^i \pmod m$ 关于 g 指标为 $\mathrm{ind}_{m,g}(x) = i \bmod \varphi(m)$ ，显然 $\mathrm{ord}_m(x) = \frac{\varphi(m)}{\gcd(\varphi(m), \mathrm{ind}_{m,g}(x))}$

离散对数与原根

- 缩系：模 m 意义下与 m 互质的元素组成缩系，缩系中任意两个元素的乘积还在缩系中，缩系的大小是 $\varphi(m)$
- 阶：满足 $x^r \equiv 1 \pmod m$ 最小正整数 r 称为 x 的阶 $\text{ord}_m(x)$
- 原根：缩系中存在元素 g 使得 g^i $(i = 1, 2, \cdots, \varphi(m))$ 两两不同，则称 g 是模 m 意义下的原根，也意味着缩系中的元素可以表示成 g 的幂次，不难得到 $\text{ord}_m(g) = \varphi(m)$
- 指标：若缩系有原根 g ，则元素 $x \equiv g^i \pmod m$ 关于 g 指标为 $\text{ind}_{m,g}(x) = i \bmod \varphi(m)$ ，显然 $\text{ord}_m(x) = \frac{\varphi(m)}{\gcd(\varphi(m), \text{ind}_{m,g}(x))}$

离散对数与原根

- 缩系：模 m 意义下与 m 互质的元素组成缩系，缩系中任意两个元素的乘积还在缩系中，缩系的大小是 $\varphi(m)$
- 阶：满足 $x^r \equiv 1 \pmod m$ 最小正整数 r 称为 x 的阶 $\text{ord}_m(x)$
- 原根：缩系中存在元素 g 使得 g^i $(i = 1, 2, \cdots, \varphi(m))$ 两两不同，则称 g 是模 m 意义下的原根，也意味着缩系中的元素可以表示成 g 的幂次，不难得到 $\text{ord}_m(g) = \varphi(m)$
- 指标：若缩系有原根 g，则元素 $x \equiv g^i \pmod m$ 关于 g 指标为 $\text{ind}_{m,g}(x) = i \bmod \varphi(m)$，显然 $\text{ord}_m(x) = \frac{\varphi(m)}{\gcd(\varphi(m), \text{ind}_{m,g}(x))}$

离散对数与原根

- 对于阶为 u 的元素 x，x^k 的阶为 $\frac{u}{\gcd(u,k)}$，所以任意元素的阶整除 $\varphi(m)$，且原根（如果存在）个数为 $\varphi(\varphi(m))$
- 这里存在一个 $\mathcal{O}(\log^2 m)$ 求阶的算法，也可用于找原根
- 缩系有原根的充要条件是 $m = 2, 4, p^n, 2p^n$，这里 p 是奇质数，n 是任意整数（证明见 David M. Burton 的 Elementary Number Theory第 8.3 节，简单易懂）
- 若缩系没有原根，则模 m 缩系可以表示成一系列有原根的缩系的笛卡儿积（图示），在 $8 \nmid m$ 时还可直接表示成生成元的幂次之积，在 $m = 2^e\ (e > 2)$ 时，5 的阶一定是 2^{e-2}

离散对数与原根

- 对于阶为 u 的元素 x，x^k 的阶为 $\frac{u}{\gcd(u,k)}$，所以任意元素的阶整除 $\varphi(m)$，且原根（如果存在）个数为 $\varphi(\varphi(m))$
- 这里存在一个 $\mathcal{O}(\log^2 m)$ 求阶的算法，也可用于找原根
- 缩系有原根的充要条件是 $m = 2, 4, p^n, 2p^n$，这里 p 是奇质数，n 是任意整数（证明见 David M. Burton 的 Elementary Number Theory第 8.3 节，简单易懂）
- 若缩系没有原根，则模 m 缩系可以表示成一系列有原根的缩系的笛卡儿积（图示），在 $8 \nmid m$ 时还可直接表示成生成元的幂次之积，在 $m = 2^e$ $(e > 2)$ 时，5 的阶一定是 2^{e-2}

离散对数与原根

- 对于阶为 u 的元素 x，x^k 的阶为 $\frac{u}{\gcd(u,k)}$，所以任意元素的阶整除 $\varphi(m)$，且原根（如果存在）个数为 $\varphi(\varphi(m))$
- 这里存在一个 $\mathcal{O}(\log^2 m)$ 求阶的算法，也可用于找原根
- 缩系有原根的充要条件是 $m = 2, 4, p^n, 2p^n$，这里 p 是奇质数，n 是任意整数（证明见 David M. Burton 的 Elementary Number Theory第 8.3 节，简单易懂）
- 若缩系没有原根，则模 m 缩系可以表示成一系列有原根的缩系的笛卡儿积（图示），在 $8 \nmid m$ 时还可直接表示成生成元的幂次之积，在 $m = 2^e$ $(e > 2)$ 时，5 的阶一定是 2^{e-2}

离散对数与原根

- 对于阶为 u 的元素 x ， x^k 的阶为 $\frac{u}{\gcd(u,k)}$ ，所以任意元素的阶整除 $\varphi(m)$ ，且原根（如果存在）个数为 $\varphi(\varphi(m))$
- 这里存在一个 $\mathcal{O}(\log^2 m)$ 求阶的算法，也可用于找原根
- 缩系有原根的充要条件是 $m = 2, 4, p^n, 2p^n$ ，这里 p 是奇质数， n 是任意整数（证明见 David M. Burton 的 Elementary Number Theory第 8.3 节，简单易懂）
- 若缩系没有原根，则模 m 缩系可以表示成一系列有原根的缩系的笛卡儿积（图示），在 $8 \nmid m$ 时还可直接表示成生成元的幂次之积，在 $m = 2^e$ $(e > 2)$ 时， 5 的阶一定是 2^{e-2}

离散对数与原根

- 考虑解方程 $A^B \equiv C \pmod M$，已知其中三个元素
- 已知 A, B, M 求 C 是模幂问题
- 已知 A, C, M 求 B 是离散对数问题
- 已知 B, C, M 求 A 是高次剩余问题
- 已知 A, B, C 求 M 是大数分解问题

离散对数与原根

- 考虑解方程 $A^B \equiv C \pmod M$，已知其中三个元素
- 已知 A, B, M 求 C 是模幂问题
- 已知 A, C, M 求 B 是离散对数问题
- 已知 B, C, M 求 A 是高次剩余问题
- 已知 A, B, C 求 M 是大数分解问题

- 解方程 $A^B \equiv C \pmod M$，已知 A, C, M 求 B，M 是质数
  - 设一个原根是 g，问题等价于 $B\text{ind}_{M,g}(A) \equiv \text{ind}_{M,g}(C) \pmod{\varphi(M)}$
  - 设 $r = \gcd(\text{ind}_{M,g}(A), \varphi(M)) = \frac{\varphi(M)}{\text{ord}_M(A)}$
    问题转化为 $B\frac{\text{ind}_{M,g}(A)}{r} \equiv \frac{\text{ind}_{M,g}(C)}{r} \pmod{\frac{\varphi(M)}{r}}$
    可得 $B \equiv \frac{\text{ind}_{M,g}(C)}{r}(\frac{\text{ind}_{M,g}(A)}{r})^{-1} \pmod{\frac{\varphi(M)}{r}}$
  - 满足 $1 \le B \le \varphi(M)$ 的解有 r 个，它们在模 $\text{ord}_M(A)$ 意义下同余，然而想算出具体值还是需要求解 $\text{ind}_{M,g}(A)$ 和 $\text{ind}_{M,g}(C)$，或者说 $\text{ind}_{M,A}(C)$

离散对数与原根

- 解方程 $A^B \equiv C \pmod M$，已知 A, C, M 求 B，M 是质数
  - 设一个原根是 g，问题等价于 $B\text{ind}_{M,g}(A) \equiv \text{ind}_{M,g}(C) \pmod{\varphi(M)}$
  - 设 $r = \gcd(\text{ind}_{M,g}(A), \varphi(M)) = \frac{\varphi(M)}{\text{ord}_M(A)}$

    问题转化为 $B\frac{\text{ind}_{M,g}(A)}{r} \equiv \frac{\text{ind}_{M,g}(C)}{r} \pmod{\frac{\varphi(M)}{r}}$

    可得 $B \equiv \frac{\text{ind}_{M,g}(C)}{r}(\frac{\text{ind}_{M,g}(A)}{r})^{-1} \pmod{\frac{\varphi(M)}{r}}$
  - 满足 $1 \le B \le \varphi(M)$ 的解有 r 个，它们在模 $\text{ord}_M(A)$ 意义下同余，然而想算出具体值还是需要求解 $\text{ind}_{M,g}(A)$ 和 $\text{ind}_{M,g}(C)$，或者说 $\text{ind}_{M,A}(C)$

离散对数与原根

- 解方程 $A^B \equiv C \pmod{M}$，已知 A, C, M 求 B，M 是质数
  - 设一个原根是 g，问题等价于 $B\mathrm{ind}_{M,g}(A) \equiv \mathrm{ind}_{M,g}(C) \pmod{\varphi(M)}$
  - 设 $r = \gcd(\mathrm{ind}_{M,g}(A), \varphi(M)) = \frac{\varphi(M)}{\mathrm{ord}_M(A)}$

    问题转化为 $B\frac{\mathrm{ind}_{M,g}(A)}{r} \equiv \frac{\mathrm{ind}_{M,g}(C)}{r} \pmod{\frac{\varphi(M)}{r}}$

    可得 $B \equiv \frac{\mathrm{ind}_{M,g}(C)}{r}(\frac{\mathrm{ind}_{M,g}(A)}{r})^{-1} \pmod{\frac{\varphi(M)}{r}}$
  - 满足 $1 \le B \le \varphi(M)$ 的解有 r 个，它们在模 $\mathrm{ord}_M(A)$ 意义下同余，然而想算出具体值还是需要求解 $\mathrm{ind}_{M,g}(A)$ 和 $\mathrm{ind}_{M,g}(C)$，或者说 $\mathrm{ind}_{M,A}(C)$

- 大步小步算法 (Baby-Step Giant-Step Algorithm)
  - 考虑求出 $1 \leq B \leq \text{ord}_M(A)$ 的唯一解，设 $B = uT - v$ ，其中 T 是设定的阈值， $1 \leq u \leq \frac{\text{ord(A)}}{T}, 0 \leq v < T$
  - 由于 A^i $(i \in \mathbb{N})$ 的轨道是一个环， $A^B \equiv C$ 可化为 $A^{uT} \equiv CA^v$
  - 预处理 A^v $(v = 0, 1, \cdots, T)$ ，枚举 u 检查是否存在解，若存在解则解唯一，故只需哈希所需的 A^v
  - 复杂度 $\mathcal{O}(T + \frac{\text{ord}_M(A)}{T})$ ，取 $T = \mathcal{O}(\sqrt{\text{ord}_M(A)})$

- 大步小步算法 (Baby-Step Giant-Step Algorithm)
  - 考虑求出 $1 \le B \le \text{ord}_M(A)$ 的唯一解，设 $B = uT - v$ ，其中 T 是设定的阈值， $1 \le u \le \frac{\text{ord(A)}}{T}, 0 \le v < T$
  - 由于 A^i $(i \in \mathbb{N})$ 的轨道是一个环， $A^B \equiv C$ 可化为 $A^{uT} \equiv CA^v$
  - 预处理 A^v $(v = 0, 1, \cdots, T)$ ，枚举 u 检查是否存在解，若存在解则解唯一，故只需哈希所需的 A^v
  - 复杂度 $\mathcal{O}(T + \frac{\text{ord}_M(A)}{T})$ ，取 $T = \mathcal{O}(\sqrt{\text{ord}_M(A)})$

离散对数与原根

- 大步小步算法 (Baby-Step Giant-Step Algorithm)
  - 考虑求出 $1 \le B \le \text{ord}_M(A)$ 的唯一解，设 $B = uT - v$ ，其中 T 是设定的阈值， $1 \le u \le \frac{\text{ord(A)}}{T}, 0 \le v < T$
  - 由于 A^i $(i \in \mathbb{N})$ 的轨道是一个环， $A^B \equiv C$ 可化为 $A^{uT} \equiv CA^v$
  - 预处理 A^v $(v = 0, 1, \cdots, T)$ ，枚举 u 检查是否存在解，若存在解则解唯一，故只需哈希所需的 A^v
  - 复杂度 $\mathcal{O}(T + \frac{\text{ord}_M(A)}{T})$ ，取 $T = \mathcal{O}(\sqrt{\text{ord}_M(A)})$

离散对数与原根

- 大步小步算法 (Baby-Step Giant-Step Algorithm)
  - 考虑求出 $1 \le B \le \text{ord}_M(A)$ 的唯一解，设 $B = uT - v$ ，其中 T 是设定的阈值， $1 \le u \le \frac{\text{ord(A)}}{T}, 0 \le v < T$
  - 由于 A^i $(i \in \mathbb{N})$ 的轨道是一个环， $A^B \equiv C$ 可化为 $A^{uT} \equiv CA^v$
  - 预处理 A^v $(v = 0, 1, \cdots, T)$ ，枚举 u 检查是否存在解，若存在解则解唯一，故只需哈希所需的 A^v
  - 复杂度 $\mathcal{O}(T + \frac{\text{ord}_M(A)}{T})$ ，取 $T = \mathcal{O}(\sqrt{\text{ord}_M(A)})$
  - 需要保证 A^i $(i \in \mathbb{N})$ 的轨道是一个环，或者说 A^{-1} 存在

离散对数与原根

- 大步小步算法 (Baby-Step Giant-Step Algorithm)
  - 考虑求出 $1 \le B \le \mathrm{ord}_M(A)$ 的唯一解，设 $B = uT - v$ ，其中 T 是设定的阈值， $1 \le u \le \frac{\mathrm{ord(A)}}{T}, 0 \le v < T$
  - 由于 A^i $(i \in \mathbb{N})$ 的轨道是一个环， $A^B \equiv C$ 可化为 $A^{uT} \equiv CA^v$
  - 预处理 A^v $(v = 0, 1, \cdots, T)$ ，枚举 u 检查是否存在解，若存在解则解唯一，故只需哈希所需的 A^v
  - 复杂度 $\mathcal{O}(T + \frac{\mathrm{ord}_M(A)}{T})$ ，取 $T = \mathcal{O}(\sqrt{\mathrm{ord}_M(A)})$
  - 需要保证 A^i $(i \in \mathbb{N})$ 的轨道是一个环，或者说 A^{-1} 存在

离散对数与原根

- 中国剩余定理：给定一系列同余方程 $x \equiv r_i \pmod{m_i}$，满足 $m_i\ (i = 1, 2, \cdots, k)$ 两两互质，则方程组存在唯一的通解 $x \equiv R \pmod{M}$，其中 $M = \mathrm{lcm}(m_1, m_2, \cdots, m_k)$, $R = \sum_{i=1}^{k} r_i {M'}_i \frac{M}{m_i}$，${M'}_i$ 表示 $\frac{M}{m_i}$ 在模 m_i 意义下乘法逆元
- 解方程 $A^B \equiv C \pmod{M}$，已知 A, C, M 求 B，满足 $\gcd(A, M) = 1$, M 是奇数（题目：数论之神）
  - 由定理可知，解在模 $\mathrm{ord}_M(A)$ 意义下唯一，大步小步算法适用

离散对数与原根

- 中国剩余定理：给定一系列同余方程 $x \equiv r_i \pmod{m_i}$，满足 $m_i\ (i = 1, 2, \cdots, k)$ 两两互质，则方程组存在唯一的通解 $x \equiv R \pmod{M}$，其中 $M = \text{lcm}(m_1, m_2, \cdots, m_k)$, $R = \sum_{i=1}^{k} r_i M'_i \frac{M}{m_i}$，$M'_i$ 表示 $\frac{M}{m_i}$ 在模 m_i 意义下乘法逆元
- 解方程 $A^B \equiv C \pmod{M}$，已知 A, C, M 求 B，满足 $\gcd(A, M) = 1$, M 是奇数（题目：数论之神）
  - 由定理可知，解在模 $\text{ord}_M(A)$ 意义下唯一，大步小步算法适用

离散对数与原根

- 中国剩余定理：给定一系列同余方程 $x \equiv r_i \pmod{m_i}$，满足 $m_i\ (i=1,2,\cdots,k)$ 两两互质，则方程组存在唯一的通解 $x \equiv R \pmod{M}$，其中 $M = \mathsf{lcm}(m_1, m_2, \cdots, m_k)$, $R = \sum_{i=1}^{k} r_i {M'}_i \frac{M}{m_i}$，${M'}_i$ 表示 $\frac{M}{m_i}$ 在模 m_i 意义下乘法逆元
- 解方程 $A^B \equiv C \pmod{M}$，已知 A, C, M 求 B，满足 $\gcd(A, M) = 1$, M 是奇数（题目：数论之神）
    - 由定理可知，解在模 $\mathsf{ord}_M(A)$ 意义下唯一，大步小步算法适用

离散对数与原根

- $\gcd(A, M) > 1$ 时，不妨考虑将 M 表示成 $\prod_{i=1}^{\omega(M)} {p_i}^{e_i}$ 的形式
- 令 $A \pmod{{p_i}^{e_i}} = {p_i}^u v$，当 $u > 0$ 时，$ut \geq e_i$ 时 $A^t \equiv 0 \pmod{{p_i}^{e_i}}$，会有一段不循环的结果，并且之后的循环节是 1，否则 $\mathrm{ord}_{{p_i}^{e_i}}(A)$ 存在，且 $\mathrm{ord}_{{p_i}^{e_i}}(A) \mid \varphi({p_i}^{e_i})$
- 经过不循环的段后，必然产生循环，循环的长度整除 $\mathrm{lcm}(\varphi({p_1}^{e_1}), \varphi({p_2}^{e_2}), \cdots, \varphi({p_{\omega(M)}}^{e_{\omega(M)}})) \mid \varphi(M)$
- 不循环的段长度小于循环的长度
- 令 $A^i \bmod M$ 向 $A^{i+1} \bmod M$ $(i \in \mathbb{N})$ 连边，轨道呈现 ρ 型

离散对数与原根

- $\gcd(A, M) > 1$ 时，不妨考虑将 M 表示成 $\prod_{i=1}^{\omega(M)} {p_i}^{e_i}$ 的形式
- 令 $A \pmod{{p_i}^{e_i}} = {p_i}^u v$ ，当 $u > 0$ 时，$ut \geq e_i$ 时 $A^t \equiv 0 \pmod{{p_i}^{e_i}}$ ，会有一段不循环的结果，并且之后的循环节是 1 ，否则 $\mathrm{ord}_{{p_i}^{e_i}}(A)$ 存在，且 $\mathrm{ord}_{{p_i}^{e_i}}(A) \mid \varphi({p_i}^{e_i})$
- 经过不循环的段后，必然产生循环，循环的长度整除 $\mathrm{lcm}(\varphi({p_1}^{e_1}), \varphi({p_2}^{e_2}), \cdots, \varphi({p_{\omega(M)}}^{e_{\omega(M)}})) \mid \varphi(M)$
- 不循环的段长度小于循环的长度
- 令 $A^i \bmod M$ 向 $A^{i+1} \bmod M$ $(i \in \mathbb{N})$ 连边，轨道呈现 ρ 型

离散对数与原根

- $\gcd(A, M) > 1$ 时，不妨考虑将 M 表示成 $\prod_{i=1}^{\omega(M)} {p_i}^{e_i}$ 的形式
- 令 $A \pmod{{p_i}^{e_i}} = {p_i}^u v$，当 $u > 0$ 时，$ut \ge e_i$ 时 $A^t \equiv 0 \pmod{{p_i}^{e_i}}$，会有一段不循环的结果，并且之后的循环节是 1，否则 $\mathrm{ord}_{{p_i}^{e_i}}(A)$ 存在，且 $\mathrm{ord}_{{p_i}^{e_i}}(A) \mid \varphi({p_i}^{e_i})$
- 经过不循环的段后，必然产生循环，循环的长度整除 $\mathrm{lcm}(\varphi({p_1}^{e_1}), \varphi({p_2}^{e_2}), \cdots, \varphi({p_{\omega(M)}}^{e_{\omega(M)}})) \mid \varphi(M)$
- 不循环的段长度小于循环的长度
- 令 $A^i \bmod M$ 向 $A^{i+1} \bmod M$ $(i \in \mathbb{N})$ 连边，轨道呈现 ρ 型

离散对数与原根

- $\gcd(A, M) > 1$ 时，不妨考虑将 M 表示成 $\prod_{i=1}^{\omega(M)} {p_i}^{e_i}$ 的形式
- 令 $A \pmod{{p_i}^{e_i}} = {p_i}^u v$ ，当 $u > 0$ 时，$ut \ge e_i$ 时 $A^t \equiv 0 \pmod{{p_i}^{e_i}}$ ，会有一段不循环的结果，并且之后的循环节是 1 ，否则 $\mathrm{ord}_{{p_i}^{e_i}}(A)$ 存在，且 $\mathrm{ord}_{{p_i}^{e_i}}(A) \mid \varphi({p_i}^{e_i})$
- 经过不循环的段后，必然产生循环，循环的长度整除 $\mathrm{lcm}(\varphi({p_1}^{e_1}), \varphi({p_2}^{e_2}), \cdots, \varphi({p_{\omega(M)}}^{e_{\omega(M)}})) \mid \varphi(M)$
- 不循环的段长度小于循环的长度
- 令 $A^i \bmod M$ 向 $A^{i+1} \bmod M$ $(i \in \mathbb{N})$ 连边，轨道呈现 ρ 型

离散对数与原根

- $\gcd(A, M) > 1$ 时，不妨考虑将 M 表示成 $\prod_{i=1}^{\omega(M)} {p_i}^{e_i}$ 的形式
- 令 $A \pmod{{p_i}^{e_i}} = {p_i}^u v$ ，当 $u > 0$ 时，$ut \geq e_i$ 时 $A^t \equiv 0 \pmod{{p_i}^{e_i}}$ ，会有一段不循环的结果，并且之后的循环节是 1 ，否则 $\mathrm{ord}_{{p_i}^{e_i}}(A)$ 存在，且 $\mathrm{ord}_{{p_i}^{e_i}}(A) \mid \varphi({p_i}^{e_i})$
- 经过不循环的段后，必然产生循环，循环的长度整除 $\mathrm{lcm}(\varphi({p_1}^{e_1}), \varphi({p_2}^{e_2}), \cdots, \varphi({p_{\omega(M)}}^{e_{\omega(M)}})) \mid \varphi(M)$
- 不循环的段长度小于循环的长度
- 令 $A^i \bmod M$ 向 $A^{i+1} \bmod M$ $(i \in \mathbb{N})$ 连边，轨道呈现 ρ 型

离散对数与原根

- Pollard's rho Algorithm for Logarithms
  - 把集合 $G = \{A^i \bmod M | i \in \mathbb{N}\}$ 分成三个部分 S_0, S_1, S_2 （比如根据模 3 的余值来划分），并保证 $1 \notin S_1$
  - 生成一系列 $x = A^i C^j$ 直到某个 x 另一种表示方法 $x = A^x C^y$ ，则 $(i - x) \equiv B(j - y) \pmod{|G|}$ ，方程可能有多解（若不在环上？）
  - 沿用 Floyd's Cycle-Finding Algorithm ，生成一系列元素 $x_0, x_1, \cdots$ 满足 $x_{i+1} = f(x_i)\ (i = 0, 1, \cdots)$ ，这里 $f(x) = Cx$ if $x \in S_0$, $f(x) = x^2$ if $x \in S_1$, $f(x) = Ax$ if $x \in S_2$
  - 维护 x_i, x_{2i} 找环，期望复杂度 $\mathcal{O}(\sqrt{\frac{\pi n}{2}})$ ，不需要 G 关于 $*$ 成循环群，证明见 Monte Carlo Methods for Index Computation $\pmod p$

离散对数与原根

- Pollard's rho Algorithm for Logarithms
  - 把集合 $G = \{A^i \bmod M | i \in \mathbb{N}\}$ 分成三个部分 S_0, S_1, S_2 （比如根据模 3 的余值来划分），并保证 $1 \notin S_1$
  - 生成一系列 $x = A^i C^j$ 直到某个 x 另一种表示方法 $x = A^x C^y$ ，则 $(i - x) \equiv B(j - y) \pmod{|G|}$ ，方程可能有多解（若不在环上？）
  - 沿用 Floyd's Cycle-Finding Algorithm ，生成一系列元素 $x_0, x_1, \cdots$ 满足 $x_{i+1} = f(x_i)$ $(i = 0, 1, \cdots)$ ，这里 $f(x) = Cx$ if $x \in S_0$, $f(x) = x^2$ if $x \in S_1$, $f(x) = Ax$ if $x \in S_2$
  - 维护 x_i, x_{2i} 找环，期望复杂度 $\mathcal{O}(\sqrt{\frac{\pi n}{2}})$ ，不需要 G 关于 $*$ 成循环群，证明见 Monte Carlo Methods for Index Computation $\pmod p$

离散对数与原根

- Pollard's rho Algorithm for Logarithms
  - 把集合 $G = \{A^i \bmod M | i \in \mathbb{N}\}$ 分成三个部分 S_0, S_1, S_2 （比如根据模 3 的余值来划分），并保证 $1 \notin S_1$
  - 生成一系列 $x = A^i C^j$ 直到某个 x 另一种表示方法 $x = A^x C^y$ ，则 $(i - x) \equiv B(j - y) \pmod{|G|}$ ，方程可能有多解（若不在环上？）
  - 沿用 Floyd's Cycle-Finding Algorithm ，生成一系列元素 $x_0, x_1, \cdots$ 满足 $x_{i+1} = f(x_i)$ $(i = 0, 1, \cdots)$ ，这里 $f(x) = Cx$ if $x \in S_0$, $f(x) = x^2$ if $x \in S_1$, $f(x) = Ax$ if $x \in S_2$
  - 维护 x_i, x_{2i} 找环，期望复杂度 $\mathcal{O}(\sqrt{\frac{\pi n}{2}})$ ，不需要 G 关于 $*$ 成循环群，证明见 Monte Carlo Methods for Index Computation $\pmod p$

离散对数与原根

- Pollard's rho Algorithm for Logarithms
  - 把集合 $G = \{A^i \bmod M | i \in \mathbb{N}\}$ 分成三个部分 S_0, S_1, S_2 （比如根据模 3 的余值来划分），并保证 $1 \notin S_1$
  - 生成一系列 $x = A^i C^j$ 直到某个 x 另一种表示方法 $x = A^x C^y$ ，则 $(i - x) \equiv B(j - y) \pmod{|G|}$ ，方程可能有多解（若不在环上？）
  - 沿用 Floyd's Cycle-Finding Algorithm ，生成一系列元素 $x_0, x_1, \cdots$ 满足 $x_{i+1} = f(x_i)$ $(i = 0, 1, \cdots)$ ，这里 $f(x) = Cx$ if $x \in S_0$, $f(x) = x^2$ if $x \in S_1$, $f(x) = Ax$ if $x \in S_2$
  - 维护 x_i, x_{2i} 找环，期望复杂度 $\mathcal{O}(\sqrt{\frac{\pi n}{2}})$ ，不需要 G 关于 $*$ 成循环群，证明见 Monte Carlo Methods for Index Computation $\pmod p$

随机函数

- 给定整数 $seed, p, n$ 和 k，求解满足方程

  $((seed^{2^x} \bmod p) \bmod n) = k$ 的最小正整数解 x，无解输出 -1
- $1 \le seed < p \le 10^9, 0 \le k < n \le 10^9$, p 是质数

随机函数

- 给定整数 $seed$, p, n 和 k ，求解满足方程

  $((seed^{2^x} \bmod p) \bmod n) = k$ 的最小正整数解 x ，无解输出 -1

- $1 \le seed < p \le 10^9, 0 \le k < n \le 10^9$, p 是质数

随机函数

- 问题可以划分成几个阶段
  - 找到 u $(0 \leq u < p)$ 满足 $u \equiv k \pmod{n}$
  - 找到 v $(1 \leq v \leq \mathrm{ord}_p(seed))$ 满足 $seed^v \equiv u \pmod{p}$
  - 找到 x $(1 \leq x \leq \mathrm{ord}_{\mathrm{ord}_p(seed)}(2)$ 满足 $2^x \equiv v \pmod{\mathrm{ord}_p(seed)}$

随机函数

- 问题可以划分成几个阶段
  - 找到 u $(0 \le u < p)$ 满足 $u \equiv k \pmod n$
  - 找到 v $(1 \le v \le \mathrm{ord}_p(seed))$ 满足 $seed^v \equiv u \pmod p$
  - 找到 x $(1 \le x \le \mathrm{ord}_{\mathrm{ord}_p(seed)}(2))$ 满足 $2^x \equiv v \pmod{\mathrm{ord}_p(seed)}$

随机函数

- 问题可以划分成几个阶段
  - 找到 u $(0 \le u < p)$ 满足 $u \equiv k \pmod n$
  - 找到 v $(1 \le v \le \mathsf{ord}_p(seed))$ 满足 $seed^v \equiv u \pmod p$
  - 找到 x $(1 \le x \le \mathsf{ord}_{\mathsf{ord}_p(seed)}(2)$ 满足 $2^x \equiv v \pmod{\mathsf{ord}_p(seed)}$

随机函数

- 问题可以划分成几个阶段
  - 找到 u $(0 \le u < p)$ 满足 $u \equiv k \pmod{n}$
  - 找到 v $(1 \le v \le \mathsf{ord}_p(seed))$ 满足 $seed^v \equiv u \pmod{p}$
  - 找到 x $(1 \le x \le \mathsf{ord}_{\mathsf{ord}_p(seed)}(2)$ 满足 $2^x \equiv v \pmod{\mathsf{ord}_p(seed)}$

随机函数

- 问题可以划分成几个阶段
  - 找到 $u\ (0 \le u < p)$ 满足 $u \equiv k \pmod{n}$
  - 找到 $v\ (1 \le v \le \mathrm{ord}_p(seed))$ 满足 $seed^v \equiv u \pmod{p}$
  - ~~找到~~$\cancel{x\ (1 \le x \le \mathrm{ord}_{\mathrm{ord}_p(seed)}(2))}$ ~~满足~~$\cancel{2^x \equiv v \pmod{\mathrm{ord}_p(seed)}}$

    $1 \le seed < p$ 且 p 是质数，所以 $\mathrm{ord}_p(seed)$ 一定存在

    但是 $\mathrm{ord}_{\mathrm{ord}_p(seed)}(2)$ 不一定存在 
  - 采用 Pollard's rho Algorithm for Logarithms 算法

随机函数

- 问题可以划分成几个阶段
  - 找到 u $(0 \leq u < p)$ 满足 $u \equiv k \pmod n$
  - 找到 v $(1 \leq v \leq \mathsf{ord}_p(seed))$ 满足 $seed^v \equiv u \pmod p$
  - ~~找到~~$\cancel{x\ (1 \leq x \leq \mathsf{ord}_{\mathsf{ord}_p(seed)}(2)}$ ~~满足~~$\cancel{2^x \equiv v \pmod{\mathsf{ord}_p(seed)}}$

    $1 \leq seed < p$ 且 p 是质数，所以 $\mathsf{ord}_p(seed)$ 一定存在

    但是 $\mathsf{ord}_{\mathsf{ord}_p(seed)}(2)$ 不一定存在
  - 采用 Pollard's rho Algorithm for Logarithms 算法

随机函数

- 问题可以划分成几个阶段
  - 找到 $u\ (0 \le u < p)$ 满足 $u \equiv k \pmod{n}$
  - 找到 $v\ (1 \le v \le \mathsf{ord}_p(seed))$ 满足 $seed^v \equiv u \pmod{p}$
  - ~~找到$x\ (1 \le x \le \mathsf{ord}_{\mathsf{ord}_p(seed)}(2))$ 满足$2^x \equiv v \pmod{\mathsf{ord}_p(seed)}$~~

    $1 \le seed < p$ 且 p 是质数，所以 $\mathsf{ord}_p(seed)$ 一定存在

    但是 $\mathsf{ord}_{\mathsf{ord}_p(seed)}(2)$ 不一定存在
  - ~~采用Pollard's rho Algorithm for Logarithms 算法~~

    最优复杂度 $\mathcal{O}(p^{\frac{3}{4}})$ ，会超过时间限制 

    不妨从 $G = \{2^i \bmod \mathsf{ord}_p(seed) | i \in \mathbb{N}\}$ 的形状入手

随机函数

- 解方程 $A^B \equiv C \pmod{M}$，已知 A, C, M 求最小非负整数 B
  - 只需最小解，若 $\gcd(A, M) = 1$，A^{-1} 有定义，大步小步算法适用
- 扩展大步小步算法 (Extended Baby-Step Giant-Step Algorithm)
  - 把方程化为 $A^{B-\delta}A^{\delta} \equiv C \pmod{M}$，消去公因子变为 $A^{B-\delta}A' \equiv C' \pmod{M'}$，枚举 $\delta = 0, 1, \cdots$ 进行下面的步骤
  - 若 $\gcd(A, M') = 1$，套用大步小步算法
  - 否则检验是否有 $A' \equiv C' \pmod{M'}$，如果有则找到解
  - 如果没有，则增加 δ，尝试将 A', C', M' 消去公因子 $\gcd(A, M')$
  - 只会进行至多 $\log_2 M$ 步消因子操作

随机函数

- 解方程 $A^B \equiv C \pmod{M}$，已知 A,C,M 求最小非负整数 B
  - 只需最小解，若 $\gcd(A,M)=1$，A^{-1} 有定义，大步小步算法适用
- 扩展大步小步算法 (Extended Baby-Step Giant-Step Algorithm)
  - 把方程化为 $A^{B-\delta}A^{\delta} \equiv C \pmod{M}$，消去公因子变为
    $A^{B-\delta}A' \equiv C' \pmod{M'}$，枚举 $\delta = 0,1,\cdots$ 进行下面的步骤
  - 若 $\gcd(A,M')=1$，套用大步小步算法
  - 否则检验是否有 $A' \equiv C' \pmod{M'}$，如果有则找到解
  - 如果没有，则增加 δ，尝试将 A',C',M' 消去公因子 $\gcd(A,M')$
  - 只会进行至多 $\log_2 M$ 步消因子操作

随机函数

- 解方程 $A^B \equiv C \pmod M$，已知 A, C, M 求最小非负整数 B
  - 只需最小解，若 $\gcd(A, M) = 1$，A^{-1} 有定义，大步小步算法适用
- 扩展大步小步算法 (Extended Baby-Step Giant-Step Algorithm)
  - 把方程化为 $A^{B-\delta}A^{\delta} \equiv C \pmod M$，消去公因子变为 $A^{B-\delta}A' \equiv C' \pmod{M'}$，枚举 $\delta = 0, 1, \cdots$ 进行下面的步骤
  - 若 $\gcd(A, M') = 1$，套用大步小步算法
  - 否则检验是否有 $A' \equiv C' \pmod{M'}$，如果有则找到解
  - 如果没有，则增加 δ，尝试将 A', C', M' 消去公因子 $\gcd(A, M')$
  - 只会进行至多 $\log_2 M$ 步消因子操作

随机函数

- 解方程 $A^B \equiv C \pmod{M}$，已知 A, C, M 求最小非负整数 B
  - 只需最小解，若 $\gcd(A, M) = 1$，A^{-1} 有定义，大步小步算法适用
- 扩展大步小步算法 (Extended Baby-Step Giant-Step Algorithm)
  - 把方程化为 $A^{B-\delta}A^{\delta} \equiv C \pmod{M}$，消去公因子变为 $A^{B-\delta}A' \equiv C' \pmod{M'}$，枚举 $\delta = 0, 1, \cdots$ 进行下面的步骤
  - 若 $\gcd(A, M') = 1$，套用大步小步算法
  - 否则检验是否有 $A' \equiv C' \pmod{M'}$，如果有则找到解
  - 如果没有，则增加 δ，尝试将 A', C', M' 消去公因子 $\gcd(A, M')$
  - 只会进行至多 $\log_2 M$ 步消因子操作

随机函数

- 解方程 $A^B \equiv C \pmod M$，已知 A, C, M 求最小非负整数 B
  - 只需最小解，若 $\gcd(A, M) = 1$，A^{-1} 有定义，大步小步算法适用
- 扩展大步小步算法 (Extended Baby-Step Giant-Step Algorithm)
  - 把方程化为 $A^{B-\delta} A^\delta \equiv C \pmod M$，消去公因子变为 $A^{B-\delta} A' \equiv C' \pmod{M'}$，枚举 $\delta = 0, 1, \cdots$ 进行下面的步骤
  - 若 $\gcd(A, M') = 1$，套用大步小步算法
  - 否则检验是否有 $A' \equiv C' \pmod{M'}$，如果有则找到解
  - 如果没有，则增加 δ，尝试将 A', C', M' 消去公因子 $\gcd(A, M')$
  - 只会进行至多 $\log_2 M$ 步消因子操作

随机函数

- 解方程 $A^B \equiv C \pmod{M}$ ，已知 A, C, M 求最小非负整数 B
  - 只需最小解，若 $\gcd(A, M) = 1$ ， A^{-1} 有定义，大步小步算法适用
- 扩展大步小步算法 (Extended Baby-Step Giant-Step Algorithm)
  - 把方程化为 $A^{B-\delta}A^{\delta} \equiv C \pmod{M}$ ，消去公因子变为 $A^{B-\delta}A' \equiv C' \pmod{M'}$ ，枚举 $\delta = 0, 1, \cdots$ 进行下面的步骤
  - 若 $\gcd(A, M') = 1$ ，套用大步小步算法
  - 否则检验是否有 $A' \equiv C' \pmod{M'}$ ，如果有则找到解
  - 如果没有，则增加 δ ，尝试将 A', C', M' 消去公因子 $\gcd(A, M')$
  - 只会进行至多 $\log_2 M$ 步消因子操作

随机函数

- 解方程 $A^B \equiv C \pmod{M}$，已知 A, C, M 求最小非负整数 B
  - 只需最小解，若 $\gcd(A, M) = 1$，A^{-1} 有定义，大步小步算法适用
- 扩展大步小步算法 (Extended Baby-Step Giant-Step Algorithm)
  - 把方程化为 $A^{B-\delta}A^{\delta} \equiv C \pmod{M}$，消去公因子变为 $A^{B-\delta}A' \equiv C' \pmod{M'}$，枚举 $\delta = 0, 1, \cdots$ 进行下面的步骤
  - 若 $\gcd(A, M') = 1$，套用大步小步算法
  - 否则检验是否有 $A' \equiv C' \pmod{M'}$，如果有则找到解
  - 如果没有，则增加 δ，尝试将 A', C', M' 消去公因子 $\gcd(A, M')$
  - 只会进行至多 $\log_2 M$ 步消因子操作

随机函数

- 解方程 $A^B \equiv C \pmod{M}$，已知 A, C, M 求最小非负整数 B
  - 只需最小解，若 $\gcd(A, M) = 1$，A^{-1} 有定义，大步小步算法适用
- 扩展大步小步算法 (Extended Baby-Step Giant-Step Algorithm)
  - 把方程化为 $A^{B-\delta}A^{\delta} \equiv C \pmod{M}$，消去公因子变为 $A^{B-\delta}A' \equiv C' \pmod{M'}$，枚举 $\delta = 0, 1, \cdots$ 进行下面的步骤
  - 若 $\gcd(A, M') = 1$，套用大步小步算法
  - 否则检验是否有 $A' \equiv C' \pmod{M'}$，如果有则找到解
  - 如果没有，则增加 δ，尝试将 A', C', M' 消去公因子 $\gcd(A, M')$
  - 只会进行至多 $\log_2 M$ 步消因子操作

随机函数

- 回到本题
  - 找到 u $(0 \leq u < p)$ 满足 $u \equiv k \pmod n$
  - 找到 v $(1 \leq v \leq \text{ord}_p(seed))$ 满足 $seed^v \equiv u \pmod p$
- 令 $\text{ord}_p(seed) = 2^e \cdot r$，求出 $\text{ord}_r(2)$，并设定阈值 Q
  - 当 $n \leq Q$ 时，枚举 $1 \leq x \leq e + \text{ord}_r(2)$ 检查，模值在模 n 意义下或可视为随机分布，期望复杂度 $O(Q)$
  - 当 $n > Q$ 时，u 有不超过 $\frac{p}{Q}$ 种取值，枚举 u 求解 v，再求解 x，期望复杂度 $O(T + \frac{p}{Q}(\log p + \frac{p}{T}))$，取 $T = O(\frac{p}{\sqrt{Q}})$
  - 为均衡两种情况的复杂度，取 $Q = O(p^{\frac{2}{3}})$

随机函数

- 回到本题
  - 找到 u $(0 \le u < p)$ 满足 $u \equiv k \pmod{n}$
  - 找到 v $(1 \le v \le \text{ord}_p(seed))$ 满足 $seed^v \equiv u \pmod{p}$
- 令 $\text{ord}_p(seed) = 2^e \cdot r$ ，求出 $\text{ord}_r(2)$ ，并设定阈值 Q
  - 当 $n \le Q$ 时，枚举 $1 \le x \le e + \text{ord}_r(2)$ 检查，模值在模 n 意义下或可视为随机分布，期望复杂度 $\mathcal{O}(Q)$
  - 当 $n > Q$ 时，u 有不超过 $\frac{p}{Q}$ 种取值，枚举 u 求解 v ，再求解 x ，期望复杂度 $\mathcal{O}(T + \frac{p}{Q}(\log p + \frac{p}{T}))$ ，取 $T = \mathcal{O}(\frac{p}{\sqrt{Q}})$
  - 为均衡两种情况的复杂度，取 $Q = \mathcal{O}(p^{\frac{2}{3}})$

随机函数

- 回到本题
  - 找到 u $(0 \le u < p)$ 满足 $u \equiv k \pmod n$
  - 找到 v $(1 \le v \le \mathrm{ord}_p(seed))$ 满足 $seed^v \equiv u \pmod p$
- 令 $\mathrm{ord}_p(seed) = 2^e \cdot r$，求出 $\mathrm{ord}_r(2)$，并设定阈值 Q
  - 当 $n \le Q$ 时，枚举 $1 \le x \le e + \mathrm{ord}_r(2)$ 检查，模值在模 n 意义下或可视为随机分布，期望复杂度 $\mathcal{O}(Q)$
  - 当 $n > Q$ 时，u 有不超过 $\frac{p}{Q}$ 种取值，枚举 u 求解 v，再求解 x，期望复杂度 $\mathcal{O}(T + \frac{p}{Q}(\log p + \frac{p}{T}))$，取 $T = \mathcal{O}(\frac{p}{\sqrt{Q}})$
  - 为均衡两种情况的复杂度，取 $Q = \mathcal{O}(p^{\frac{2}{3}})$

随机函数

- 回到本题
  - 找到 u $(0 \le u < p)$ 满足 $u \equiv k \pmod{n}$
  - 找到 v $(1 \le v \le \mathrm{ord}_p(seed))$ 满足 $seed^v \equiv u \pmod{p}$
- 令 $\mathrm{ord}_p(seed) = 2^e \cdot r$ ，求出 $\mathrm{ord}_r(2)$ ，并设定阈值 Q
  - 当 $n \le Q$ 时，枚举 $1 \le x \le e + \mathrm{ord}_r(2)$ 检查，模值在模 n 意义下或可视为随机分布，期望复杂度 $\mathcal{O}(Q)$
  - 当 $n > Q$ 时，u 有不超过 $\frac{p}{Q}$ 种取值，枚举 u 求解 v ，再求解 x ，期望复杂度 $\mathcal{O}(T + \frac{p}{Q}(\log p + \frac{p}{T}))$ ，取 $T = \mathcal{O}(\frac{p}{\sqrt{Q}})$
  - 为均衡两种情况的复杂度，取 $Q = \mathcal{O}(p^{\frac{2}{3}})$

随机函数

- 回到本题
  - 找到 u $(0 \le u < p)$ 满足 $u \equiv k \pmod{n}$
  - 找到 v $(1 \le v \le \mathrm{ord}_p(seed))$ 满足 $seed^v \equiv u \pmod{p}$
- 令 $\mathrm{ord}_p(seed) = 2^e \cdot r$ ，求出 $\mathrm{ord}_r(2)$ ，并设定阈值 Q
  - 当 $n \le Q$ 时，枚举 $1 \le x \le e + \mathrm{ord}_r(2)$ 检查，模值在模 n 意义下或可视为随机分布，期望复杂度 $\mathcal{O}(Q)$
  - 当 $n > Q$ 时，u 有不超过 $\frac{p}{Q}$ 种取值，枚举 u 求解 v ，再求解 x ，期望复杂度 $\mathcal{O}(T + \frac{p}{Q}(\log p + \frac{p}{T}))$ ，取 $T = \mathcal{O}(\frac{p}{\sqrt{Q}})$
  - 为均衡两种情况的复杂度，取 $Q = \mathcal{O}(p^{\frac{2}{3}})$

$A^B \bmod M$

- 给定整数 B, C 和 M ，求解满足方程 $A^B \equiv C \pmod{M}$ 且 $A \le M$ 的所有非负整数解 A ，无解输出 No Solution
- 保证解的数量不超过 $\sqrt{M}$
- $1 \le B, C < M \le 10^9$

$A^B \bmod M$

- 给定整数 B, C 和 M ，求解满足方程 $A^B \equiv C \pmod{M}$ 且 $A \le M$ 的所有非负整数解 A ，无解输出 No Solution
- 保证解的数量不超过 $\sqrt{M}$
- $1 \le B, C < M \le 10^9$

$A^B \bmod M$

- 给定整数 B, C 和 M，求解满足方程 $A^B \equiv C \pmod{M}$ 且 $A \leq M$ 的所有非负整数解 A，无解输出 No Solution
- 保证解的数量不超过 $\sqrt{M}$
- $1 \leq B, C < M \leq 10^9$

$A^B \bmod M$

- 解方程 $A^B \equiv C \pmod{M}$，已知 B, C, M 求 A
  - 高次剩余问题
  - M 有原根时问题会好办许多，考虑 M 是质数幂次的情况，然后利用中国剩余定理合并
  - $M = 2^e$ 时没有原根，需要完善做法

$A^B \bmod M$

- 解方程 $A^B \equiv C \pmod M$，已知 B, C, M 求 A
  - 高次剩余问题
  - M 有原根时问题会好办许多，考虑 M 是质数幂次的情况，然后利用中国剩余定理合并
  - $M = 2^e$ 时没有原根，需要完善做法

$A^B \bmod M$

- 解方程 $A^B \equiv C \pmod{M}$，已知 B, C, M 求 A
  - 高次剩余问题
  - M 有原根时问题会好办许多，考虑 M 是质数幂次的情况，然后利用中国剩余定理合并
  - $M = 2^e$ 时没有原根，需要完善做法

$A^B \bmod M$

- 解高次剩余 $A^B \equiv C \pmod{M}$, $M = p^e$, p 是奇质数
  - 若 $C \equiv 0 \pmod{M}$，则 $x = p^u v$ $(\gcd(p, v) = 1)$ 满足 $uB \geq e$ 即可，即 $p^{\lceil \frac{e}{B} \rceil} \mid x$
  - 若 $\gcd(C, M) = 1$，可以取一原根 g 将问题转化为 $B\mathsf{ind}_{M,g}(x) \equiv \mathsf{ind}_{M,g}(C) \pmod{\varphi(M)}$，消公因子后检查是否有解，有解则利用扩展欧几里得算法求出通解即可
  - 若 $1 < \gcd(C, M) < M$，令 $C = p^a b$ $(\gcd(a, b) = 1)$，那么 $B \mid a$, $p^{\frac{a}{B}} \mid x$，消因子后转化为 $\gcd(C, M) = 1$ 的情况，转化回来时需要扩张解的所在域（例子）

$A^B \bmod M$

- 解高次剩余 $A^B \equiv C \pmod{M}$, $M = p^e$, p 是奇质数
  - 若 $C \equiv 0 \pmod{M}$，则 $x = p^u v$ $(\gcd(p, v) = 1)$ 满足 $uB \geq e$ 即可，即 $p^{\lceil \frac{e}{B} \rceil} \mid x$
  - 若 $\gcd(C, M) = 1$，可以取一原根 g 将问题转化为 $B\mathrm{ind}_{M,g}(x) \equiv \mathrm{ind}_{M,g}(C) \pmod{\varphi(M)}$，消公因子后检查是否有解，有解则利用扩展欧几里得算法求出通解即可
  - 若 $1 < \gcd(C, M) < M$，令 $C = p^a b$ $(\gcd(a, b) = 1)$，那么 $B \mid a$, $p^{\frac{a}{B}} \mid x$，消因子后转化为 $\gcd(C, M) = 1$ 的情况，转化回来时需要扩张解的所在域（例子）

- 解高次剩余 $A^B \equiv C \pmod{M}$, $M = p^e$, p 是奇质数
  - 若 $C \equiv 0 \pmod{M}$，则 $x = p^u v\ (\gcd(p, v) = 1)$ 满足 $uB \geq e$ 即可，即 $p^{\lceil \frac{e}{B} \rceil} \mid x$
  - 若 $\gcd(C, M) = 1$，可以取一原根 g 将问题转化为 $B\mathrm{ind}_{M,g}(x) \equiv \mathrm{ind}_{M,g}(C) \pmod{\varphi(M)}$，消公因子后检查是否有解，有解则利用扩展欧几里得算法求出通解即可
  - 若 $1 < \gcd(C, M) < M$，令 $C = p^a b\ (\gcd(a, b) = 1)$，那么 $B \mid a$, $p^{\frac{a}{B}} \mid x$，消因子后转化为 $\gcd(C, M) = 1$ 的情况，转化回来时需要扩张解的所在域（例子）

$A^B \bmod M$

- 解高次剩余 $A^B \equiv C \pmod M, M = 2^e$
  - 当 $e > 2$ 时缩系可以表示成两个循环群的直和 $C_2 \times C_{2^{e-2}}$，然而没有办法使用中国剩余定理
  - 看到解的数量不超过 $\sqrt{M}$，一个暴力的想法是生成出所有的解
  - 如果有 $A^B \equiv C \pmod{2^e}$，那么一定有 $A^B \equiv C \pmod{2^{e-1}}$
  - 假设已知 $x^B \equiv C \pmod{2^{e-1}}$，那么可能有 $x^B \equiv C \pmod{2^e}$ 或 $(x + 2^{e-1})^B \equiv C \pmod{2^e}$，利用这个必要条件进行 BFS 即可

$A^B \bmod M$

- 解高次剩余 $A^B \equiv C \pmod{M}, M = 2^e$
  - 当 $e > 2$ 时缩系可以表示成两个循环群的直和 $C_2 \times C_{2^{e-2}}$ ，然而没有办法使用中国剩余定理
  - 看到解的数量不超过 $\sqrt{M}$ ，一个暴力的想法是生成出所有的解
  - 如果有 $A^B \equiv C \pmod{2^e}$ ，那么一定有 $A^B \equiv C \pmod{2^{e-1}}$
  - 假设已知 $x^B \equiv C \pmod{2^{e-1}}$ ，那么可能有 $x^B \equiv C \pmod{2^e}$ 或 $(x + 2^{e-1})^B \equiv C \pmod{2^e}$ ，利用这个必要条件进行 BFS 即可

- 解高次剩余 $A^B \equiv C \pmod{M}$, $M = 2^e$
  - 当 $e > 2$ 时缩系可以表示成两个循环群的直和 $C_2 \times C_{2^{e-2}}$，然而没有办法使用中国剩余定理
  - 看到解的数量不超过 $\sqrt{M}$，一个暴力的想法是生成出所有的解
  - 如果有 $A^B \equiv C \pmod{2^e}$，那么一定有 $A^B \equiv C \pmod{2^{e-1}}$
  - 假设已知 $x^B \equiv C \pmod{2^{e-1}}$，那么可能有 $x^B \equiv C \pmod{2^e}$ 或 $(x + 2^{e-1})^B \equiv C \pmod{2^e}$，利用这个必要条件进行 BFS 即可

$A^B \bmod M$

- 解高次剩余 $A^B \equiv C \pmod M$, $M = 2^e$
  - 当 $e > 2$ 时缩系可以表示成两个循环群的直和 $C_2 \times C_{2^{e-2}}$，然而没有办法使用中国剩余定理
  - 看到解的数量不超过 $\sqrt{M}$，一个暴力的想法是生成出所有的解
  - 如果有 $A^B \equiv C \pmod{2^e}$，那么一定有 $A^B \equiv C \pmod{2^{e-1}}$
  - 假设已知 $x^B \equiv C \pmod{2^{e-1}}$，那么可能有 $x^B \equiv C \pmod{2^e}$ 或 $(x + 2^{e-1})^B \equiv C \pmod{2^e}$，利用这个必要条件进行 BFS 即可
  - 由于模 2^e 意义的特殊性，这个方法是可以通过的，直到有一天昨天我又翻了一遍《数论讲义》……

$A^B \bmod M$

- 解高次剩余 $A^B \equiv C \pmod{M}, M = 2^e$
  - 当 $e > 2$ 时缩系可以表示成两个循环群的直和 $C_2 \times C_{2^{e-2}}$ ，然而没有办法使用中国剩余定理
  - 看到解的数量不超过 $\sqrt{M}$ ，一个暴力的想法是生成出所有的解
  - 如果有 $A^B \equiv C \pmod{2^e}$ ，那么一定有 $A^B \equiv C \pmod{2^{e-1}}$
  - 假设已知 $x^B \equiv C \pmod{2^{e-1}}$ ，那么可能有 $x^B \equiv C \pmod{2^e}$ 或 $(x + 2^{e-1})^B \equiv C \pmod{2^e}$ ，利用这个必要条件进行 BFS 即可
  - 由于模 2^e 意义的特殊性，这个方法是可以通过的，直到~~有一天~~昨天我又翻了一遍《数论讲义》……

震惊!

模 2^e 意义也有"原根"!

$A^B \bmod M$

- 当 $e > 2$ 时，可以归纳证明 $5^{2^{e-3}} \equiv 1 + 2^{e-1} \pmod{2^e}$，从而得到 $\mathrm{ord}_{2^e}(5) = 2^{e-2}$
- 这意味着 5 的幂次可以生成 2^{e-2} 个形如 $4k+1$ 的数字，而缩系中恰好有 2^{e-2} 个形如 $4k+1$ 的数字
- 形如 $4k+1$ 的数字乘以 (-1) 即可生成剩下的 2^{e-2} 个与 2^e 互质的数字，它们都是 $4k+3$ 的形式
- 对于 $\gcd(A, 2^e) = 1$ 的情况，有 $A \equiv (-1)^{\frac{A-1}{2}} 5^u \pmod{2^e}$，根据 B 的奇偶性讨论一下即可转化为离散对数问题，不用受解数的限制

$A^B \bmod M$

- 当 $e > 2$ 时，可以归纳证明 $5^{2^{e-3}} \equiv 1 + 2^{e-1} \pmod{2^e}$，从而得到 $\mathrm{ord}_{2^e}(5) = 2^{e-2}$
- 这意味着 5 的幂次可以生成 2^{e-2} 个形如 $4k+1$ 的数字，而缩系中恰好有 2^{e-2} 个形如 $4k+1$ 的数字
- 形如 $4k+1$ 的数字乘以 (-1) 即可生成剩下的 2^{e-2} 个与 2^e 互质的数字，它们都是 $4k+3$ 的形式
- 对于 $\gcd(A, 2^e) = 1$ 的情况，有 $A \equiv (-1)^{\frac{A-1}{2}} 5^u \pmod{2^e}$，根据 B 的奇偶性讨论一下即可转化为离散对数问题，不用受解数的限制

$A^B \bmod M$

- 当 $e > 2$ 时，可以归纳证明 $5^{2^{e-3}} \equiv 1 + 2^{e-1} \pmod{2^e}$，从而得到 $\mathrm{ord}_{2^e}(5) = 2^{e-2}$
- 这意味着 5 的幂次可以生成 2^{e-2} 个形如 $4k+1$ 的数字，而缩系中恰好有 2^{e-2} 个形如 $4k+1$ 的数字
- 形如 $4k+1$ 的数字乘以 (-1) 即可生成剩下的 2^{e-2} 个与 2^e 互质的数字，它们都是 $4k+3$ 的形式
- 对于 $\gcd(A, 2^e) = 1$ 的情况，有 $A \equiv (-1)^{\frac{A-1}{2}} 5^u \pmod{2^e}$，根据 B 的奇偶性讨论一下即可转化为离散对数问题，不用受解数的限制

$A^B \bmod M$

- 当 $e > 2$ 时，可以归纳证明 $5^{2^{e-3}} \equiv 1 + 2^{e-1} \pmod{2^e}$，从而得到 $\mathrm{ord}_{2^e}(5) = 2^{e-2}$
- 这意味着 5 的幂次可以生成 2^{e-2} 个形如 $4k+1$ 的数字，而缩系中恰好有 2^{e-2} 个形如 $4k+1$ 的数字
- 形如 $4k+1$ 的数字乘以 (-1) 即可生成剩下的 2^{e-2} 个与 2^e 互质的数字，它们都是 $4k+3$ 的形式
- 对于 $\gcd(A, 2^e) = 1$ 的情况，有 $A \equiv (-1)^{\frac{A-1}{2}} 5^u \pmod{2^e}$，根据 B 的奇偶性讨论一下即可转化为离散对数问题，不用受解数的限制

离散对数与原根

- Summarize
  - 掉线的同学可以准备重连了
  - 大步小步算法是分块算法中的经典算法，使用时可以记住一点

    一次使用，多次受用
  - 通过原根可以将问题降低层次，或许会转化为更简单的问题，例如

    简单离散对数问题转化为高次剩余后可以降低复杂度
  - 高次剩余问题是一个不比离散对数问题难的问题
  - 扩张域的技巧有时很有用（循环探求、模意义贝尔数、模意义斐波

    那契数等）

离散对数与原根

- Summarize
  - ~~掉线的同学可以准备重连了~~ 学习使我快乐
  - 大步小步算法是分块算法中的经典算法，使用时可以记住一点
    一次使用，多次受用
  - 通过原根可以将问题降低层次，或许会转化为更简单的问题，例如简单离散对数问题转化为高次剩余后可以降低复杂度
  - 高次剩余问题是一个不比离散对数问题难的问题
  - 扩张域的技巧有时很有用（循环探求、模意义贝尔数、模意义斐波那契数等）

- Summarize
  - ~~掉线的同学可以准备重连了~~ 学习使我快乐
  - 大步小步算法是分块算法中的经典算法，使用时可以记住一点
    一次使用，多次受用
  - 通过原根可以将问题降低层次，或许会转化为更简单的问题，例如
    简单离散对数问题转化为高次剩余后可以降低复杂度
  - 高次剩余问题是一个不比离散对数问题难的问题
  - 扩张域的技巧有时很有用（循环探求、模意义贝尔数、模意义斐波那契数等）

离散对数与原根

- Summarize
  - ~~掉线的同学可以准备重连了~~ 学习使我快乐
  - 大步小步算法是分块算法中的经典算法，使用时可以记住一点
    一次使用，多次受用
  - 通过原根可以将问题降低层次，或许会转化为更简单的问题，例如
    简单离散对数问题转化为高次剩余后可以降低复杂度
  - 高次剩余问题是一个不比离散对数问题难的问题
  - 扩张域的技巧有时很有用（循环探求、模意义贝尔数、模意义斐波那契数等）

离散对数与原根

- Summarize
  - ~~掉线的同学可以准备重连了~~ 学习使我快乐
  - 大步小步算法是分块算法中的经典算法，使用时可以记住一点

    一次使用，多次受用
  - 通过原根可以将问题降低层次，或许会转化为更简单的问题，例如

    简单离散对数问题转化为高次剩余后可以降低复杂度
  - 高次剩余问题是一个不比离散对数问题难的问题
  - 扩张域的技巧有时很有用（循环探求、模意义贝尔数、模意义斐波

    那契数等）

互动交流

- Feel free to ask any questions

感谢

感谢工作人员提供技术支持

感谢听课的各位的积极参与

祝大家在学习训练中有所收获，在比赛考试中旗开得胜

祝 51nod 越办越好

感谢

感谢工作人员提供技术支持

感谢听课的各位的积极参与

祝大家在学习训练中有所收获，在比赛考试中旗开得胜

祝 51nod 越办越好

感谢

感谢工作人员提供技术支持

感谢听课的各位的积极参与

祝大家在学习训练中有所收获，在比赛考试中旗开得胜

祝 51nod 越办越好

感谢

感谢工作人员提供技术支持

感谢听课的各位的积极参与

祝大家在学习训练中有所收获，在比赛考试中旗开得胜

祝 51nod 越办越好

感谢又善良，又仁慈，又有钱的夹克老爷

感谢

感谢工作人员提供技术支持

感谢听课的各位的积极参与

祝大家在学习训练中有所收获，在比赛考试中旗开得胜

祝 51nod 越办越好

感谢又善良，又仁慈，又有钱的夹克老爷