算法竞赛中的数学问题——例题

东北育才学校　张听海

February 5, 2018

1. 因数与倍数
   - 例 1. [UOJ48] 核聚变反应强度
   - 例 2. [POJ3696] The Luckiest Number
2. 欧拉函数
3. 三分法

1 因数与倍数
- 例 1. [UOJ48] 核聚变反应强度
- 例 2. [POJ3696] The Luckiest Number

2 欧拉函数

3 三分法

例 1. [UOJ48] 核聚变反应强度

给出 n 个正整数 $a_1, a_2, \cdots, a_n$，计算 a_1 与每个 a_i 的次大公约数（能同时整除 x, y 的正整数中第二大的数），如果没有输出 -1.

例 1. [UOJ48] 核聚变反应强度

给出 n 个正整数 $a_1,a_2,\cdots,a_n$，计算 a_1 与每个 a_i 的次大公约数（能同时整除 x,y 的正整数中第二大的数），如果没有输出 -1.
$n \leqslant 10^5$，$a_i \leqslant 10^{12}$.

例 1. [UOJ48] 核聚变反应强度

给出 n 个正整数 $a_1, a_2, \cdots, a_n$，计算 a_1 与每个 a_i 的次大公约数（能同时整除 x, y 的正整数中第二大的数），如果没有输出 -1.
$n \leqslant 10^5$，$a_i \leqslant 10^{12}$.

对于两个正整数 a_1 和 a_i，它们的公约数必为 $\gcd(a_1, a_i)$ 的公约数. 即求 $\gcd(a_1, a_i)$ 的次大公约数.

例 1. [UOJ48] 核聚变反应强度

给出 n 个正整数 $a_1, a_2, \cdots, a_n$，计算 a_1 与每个 a_i 的次大公约数（能同时整除 x, y 的正整数中第二大的数），如果没有输出 -1.
$n \leqslant 10^5$，$a_i \leqslant 10^{12}$.

对于两个正整数 a_1 和 a_i，它们的公约数必为 $\gcd(a_1, a_i)$ 的公约数.
即求 $\gcd(a_1, a_i)$ 的次大公约数.
欧拉筛预处理出质数数列.

例 1. [UOJ48] 核聚变反应强度

给出 n 个正整数 $a_1,a_2,\cdots,a_n$，计算 a_1 与每个 a_i 的次大公约数（能同时整除 x,y 的正整数中第二大的数），如果没有输出 -1.
$n \leqslant 10^5$，$a_i \leqslant 10^{12}$.

对于两个正整数 a_1 和 a_i，它们的公约数必为 $\gcd(a_1,a_i)$ 的公约数.
即求 $\gcd(a_1,a_i)$ 的次大公约数.
欧拉筛预处理出质数数列.
对于每个 a_i，欧几里得算法求出 $\gcd(a_1,a_i)$，之后从小到大用质数试除，找到最小的 $p \mid \gcd(a_1,a_i)$，输出 $\dfrac{\gcd(a_1,a_i)}{p}$.

1. 因数与倍数
   - 例 1. [UOJ48] 核聚变反应强度
   - 例 2. [POJ3696] The Luckiest Number
2. 欧拉函数
3. 三分法

例 2. [POJ3696] The Luckiest Number

对于给定的整数 L, 找出 L 能整除最短的全 8 序列的长度.

例 2. [POJ3696] The Luckiest Number

对于给定的整数 L, 找出 L 能整除最短的全 8 序列的长度.

注: 全 8 序列为形如 $\underbrace{888\cdots8}_{n\text{个}8}$.

例 2. [POJ3696] The Luckiest Number

对于给定的整数 L, 找出 L 能整除最短的全 8 序列的长度.

注: 全 8 序列为形如 $\underbrace{888\cdots8}_{n\text{个}8}$.

多组数据.

例 2. [POJ3696] The Luckiest Number

对于给定的整数 L, 找出 L 能整除最短的全 8 序列的长度.

注: 全 8 序列为形如 $\underbrace{888\cdots8}_{n\text{个}8}$.

多组数据.

$1 \leqslant L \leqslant 2\times10^9$.

例 2. [POJ3696] The Luckiest Number

对于给定的整数 L，找出 L 能整除最短的全 8 序列的长度.

注：全 8 序列为形如 $\underbrace{888\cdots8}_{n个8}$.

多组数据.

$1 \leqslant L \leqslant 2 \times 10^9$.

$$\underbrace{888\cdots8}_{n个8} = \frac{8}{9}\left(10^n - 1\right) = L \cdot p, \text{ 即 } 10^x - 1 = \frac{9Lp}{8}.$$

例 2. [POJ3696] The Luckiest Number

对于给定的整数 L，找出 L 能整除最短的全 8 序列的长度.

注：全 8 序列为形如 $\underbrace{888\cdots8}_{n\text{个}8}$.

多组数据.

$1 \leqslant L \leqslant 2\times10^9$.

$\underbrace{888\cdots8}_{n\text{个}8} = \frac{8}{9}\left(10^n-1\right) = L\cdot p$，即 $10^x-1=\frac{9Lp}{8}$.

设 $m=\frac{9L}{\gcd(L,8)}$，则存在 p' 使得 $10^x-1=mp'$，即求 $10^x\equiv1 \pmod m$ 的最小解.

例 2. [POJ3696] The Luckiest Number

对于给定的整数 L, 找出 L 能整除最短的全 8 序列的长度.
注: 全 8 序列为形如 $\underbrace{888\cdots8}_{n个8}$.
多组数据.
$1 \leqslant L \leqslant 2\times10^9$.

$\underbrace{888\cdots8}_{n个8} = \frac{8}{9}\left(10^n-1\right) = L\cdot p$, 即 $10^x-1 = \frac{9Lp}{8}$.

设 $m = \frac{9L}{\gcd(L,8)}$, 则存在 p' 使得 $10^x-1 = mp'$, 即求 $10^x \equiv 1 \pmod m$ 的最小解.

当 $\gcd(10,m)\neq 1$ 时, 无解.

例 2. [POJ3696] The Luckiest Number

当 $\gcd(10, m) = 1$ 时, 由于 $10^{\varphi(m)} \equiv 1 \pmod m$, 只需考虑 $\varphi(m)$ 的因子.

例 2. [POJ3696] The Luckiest Number

当 $\gcd(10, m) = 1$ 时, 由于 $10^{\varphi(m)} \equiv 1 \pmod m$, 只需考虑 $\varphi(m)$ 的因子.

对 $\varphi(m)$ 质因数分解.

例 2. [POJ3696] The Luckiest Number

当 $\gcd(10, m) = 1$ 时, 由于 $10^{\varphi(m)} \equiv 1 \pmod{m}$, 只需考虑 $\varphi(m)$ 的因子.

对 $\varphi(m)$ 质因数分解.

对每个质因子 p_i, 执行 $n = n/p_i$ 直到以下情形之一被满足:

(1) $p_i \nmid n$; (2) $x^n \not\equiv 1 \pmod{m}$.

例 2. [POJ3696] The Luckiest Number

当 $\gcd(10, m) = 1$ 时，由于 $10^{\varphi(m)} \equiv 1 \pmod m$，只需考虑 $\varphi(m)$ 的因子.

对 $\varphi(m)$ 质因数分解.

对每个质因子 p_i，执行 $n = n/p_i$ 直到以下情形之一被满足：

(1) $p_i \nmid n$；(2) $x^n \not\equiv 1 \pmod m$.

考虑过全部质因子后即得解.

1 因数与倍数

2 欧拉函数

- 例 3. [BZOJ2818]Gcd
- 例 4. [BZOJ3884] 上帝与集合的正确用法
- 例 5. 离散对数问题

3 三分法

1 因数与倍数

2 欧拉函数

- 例 3. [BZOJ2818]Gcd
- 例 4. [BZOJ3884] 上帝与集合的正确用法
- 例 5. 离散对数问题

3 三分法

例 3. [BZOJ2818]Gcd

给定整数 N, 求 $1 \leqslant x,y \leqslant N$ 且 $\gcd(x,y)$ 为素数的数对 (x,y) 有多少对?

例 3. [BZOJ2818]Gcd

给定整数 N, 求 $1 \leqslant x,y \leqslant N$ 且 $\gcd(x,y)$ 为素数的数对 (x,y) 有多少对?

$1 \leqslant N \leqslant 10^7$.

例 3. [BZOJ2818]Gcd

给定整数 N, 求 $1 \leqslant x, y \leqslant N$ 且 $\gcd(x, y)$ 为素数的数对 (x, y) 有多少对?
$1 \leqslant N \leqslant 10^7$.

欧拉筛法预处理质数数列及 $\varphi(n)$ 前缀和.

例 3. [BZOJ2818]Gcd

给定整数 N, 求 $1 \leqslant x,y \leqslant N$ 且 $\gcd(x,y)$ 为素数的数对 (x,y) 有多少对?
$1 \leqslant N \leqslant 10^7$.

欧拉筛法预处理质数数列及 $\varphi(n)$ 前缀和.
题目等价于求 $1 \leqslant x,y \leqslant \left\lfloor \frac{N}{p} \right\rfloor$ 且 $\gcd(x,y) = 1$ 的数对的个数, 其中 p 为质数.

1 因数与倍数

2 欧拉函数

- 例 3. [BZOJ2818]Gcd
- 例 4. [BZOJ3884] 上帝与集合的正确用法
- 例 5. 离散对数问题

3 三分法

例 4. [BZOJ3884] 上帝与集合的正确用法

求 $2^{2^{2^{2^{\cdots}}}} \bmod p$ 的值.

例 4. [BZOJ3884] 上帝与集合的正确用法

求 $2^{2^{2^{\cdots}}} \mod p$ 的值.

T 组数据.

例 4. [BZOJ3884] 上帝与集合的正确用法

求 $2^{2^{2^{\cdots}}} \bmod p$ 的值.

T 组数据.

$T \leqslant 1,000$，$1 \leqslant p \leqslant 10^7$.

例 4. [BZOJ3884] 上帝与集合的正确用法

求 $2^{2^{2^{\cdots}}} \bmod p$ 的值.

T 组数据.

$T \leqslant 1,000$，$1 \leqslant p \leqslant 10^7$.

欧拉筛预处理欧拉函数值.

例 4. [BZOJ3884] 上帝与集合的正确用法

求 $2^{2^{2^{\cdots}}} \bmod p$ 的值.

T 组数据.

$T \leqslant 1,000$, $1 \leqslant p \leqslant 10^7$.

欧拉筛预处理欧拉函数值.

设 $p = 2^k \cdot q$, 其中 q 为奇数. 则 $2^{2^{2^{\cdots}}} \bmod p = 2^k \left(2^{2^{2^{\cdots}}-k} \bmod q \right)$.

例 4. [BZOJ3884] 上帝与集合的正确用法

求 $2^{2^{2^{\cdots}}} \bmod p$ 的值.
T 组数据.
$T \leqslant 1,000$，$1 \leqslant p \leqslant 10^7$.

欧拉筛预处理欧拉函数值.
设 $p = 2^k \cdot q$，其中 q 为奇数. 则 $2^{2^{2^{\cdots}}} \bmod p = 2^k \left(2^{2^{2^{\cdots}}-k} \bmod q\right)$.
由欧拉定理 $2^k \left(2^{2^{2^{\cdots}}-k} \bmod q\right) = 2^k \left[2^{\left(2^{2^{\cdots}}-k\right) \bmod \varphi(q)} \bmod q\right]$.

例 4. [BZOJ3884] 上帝与集合的正确用法

求 $2^{2^{2^{\cdots}}} \bmod p$ 的值.

T 组数据.

$T \leqslant 1,000$, $1 \leqslant p \leqslant 10^7$.

欧拉筛预处理欧拉函数值.

设 $p = 2^k \cdot q$, 其中 q 为奇数. 则 $2^{2^{2^{\cdots}}} \bmod p = 2^k \left(2^{2^{2^{\cdots}}-k} \bmod q\right)$.

由欧拉定理 $2^k \left(2^{2^{2^{\cdots}}-k} \bmod q\right) = 2^k \left[2^{\left(2^{2^{\cdots}}-k\right) \bmod \varphi(q)} \bmod q\right]$.

递归计算, 直至 $q = 1$.

1 因数与倍数

2 欧拉函数

- 例 3. [BZOJ2818]Gcd
- 例 4. [BZOJ3884] 上帝与集合的正确用法
- 例 5. 离散对数问题

3 三分法

例 5. 离散对数问题

已知 a, b, n, 解同余方程 $a^x \equiv b \pmod{n}$, 其中 $\gcd(a, n) = 1$.

例 5. 离散对数问题

已知 a,b,n，解同余方程 $a^x \equiv b \pmod n$，其中 $\gcd(a,n)=1$.

由欧拉定理，$a^x \equiv a^{x+\varphi(n)} \pmod n$. 因此只需枚举 $0 \leqslant x < \varphi(n)$.

例 5. 离散对数问题

已知 a,b,n，解同余方程 $a^x \equiv b \pmod{n}$，其中 $\gcd(a,n)=1$.

由欧拉定理，$a^x \equiv a^{x+\varphi(n)} \pmod{n}$. 因此只需枚举 $0 \leqslant x < \varphi(n)$.
分块优化. 设 $x = p\left\lceil \sqrt{\varphi(n)} \right\rceil - q$，这里 $0 < p,q \leqslant \left\lceil \sqrt{\varphi(n)} \right\rceil$.

例 5. 离散对数问题

已知 a,b,n，解同余方程 $a^x \equiv b \pmod n$，其中 $\gcd(a,n)=1$.

由欧拉定理，$a^x \equiv a^{x+\varphi(n)} \pmod n$. 因此只需枚举 $0 \leqslant x < \varphi(n)$.
分块优化. 设 $x = p\left\lceil\sqrt{\varphi(n)}\right\rceil - q$，这里 $0 < p,q \leqslant \left\lceil\sqrt{\varphi(n)}\right\rceil$.
则 $a^{p\lceil\sqrt{\varphi(n)}\rceil - q} \equiv b \pmod n$ 等价于 $a^{p\lceil\sqrt{\varphi(n)}\rceil} \equiv b \cdot a^q \pmod n$.

例 5. 离散对数问题

已知 a, b, n, 解同余方程 $a^x \equiv b \pmod{n}$, 其中 $\gcd(a, n) = 1$.

由欧拉定理, $a^x \equiv a^{x+\varphi(n)} \pmod{n}$. 因此只需枚举 $0 \leqslant x < \varphi(n)$.

分块优化. 设 $x = p\left\lceil\sqrt{\varphi(n)}\right\rceil - q$, 这里 $0 < p, q \leqslant \left\lceil\sqrt{\varphi(n)}\right\rceil$.

则 $a^{p\lceil\sqrt{\varphi(n)}\rceil - q} \equiv b \pmod{n}$ 等价于 $a^{p\lceil\sqrt{\varphi(n)}\rceil} \equiv b \cdot a^q \pmod{n}$.

枚举 $0 < q \leqslant \left\lceil\sqrt{\varphi(n)}\right\rceil$, 用 hash 表记录余数与 q 值的关系.

例 5. 离散对数问题

已知 a,b,n，解同余方程 $a^x \equiv b \pmod{n}$，其中 $\gcd(a,n)=1$.

由欧拉定理，$a^x \equiv a^{x+\varphi(n)} \pmod{n}$. 因此只需枚举 $0 \leqslant x < \varphi(n)$.

分块优化. 设 $x = p\left\lceil\sqrt{\varphi(n)}\right\rceil - q$，这里 $0 < p,q \leqslant \left\lceil\sqrt{\varphi(n)}\right\rceil$.

则 $a^{p\lceil\sqrt{\varphi(n)}\rceil - q} \equiv b \pmod{n}$ 等价于 $a^{p\lceil\sqrt{\varphi(n)}\rceil} \equiv b \cdot a^q \pmod{n}$.

枚举 $0 < q \leqslant \left\lceil\sqrt{\varphi(n)}\right\rceil$，用 hash 表记录余数与 q 值的关系.

再枚举 p，找到使 x 最小的 p,q.

例 5. 离散对数问题

已知 a,b,n，解同余方程 $a^x \equiv b \pmod{n}$，其中 $\gcd(a,n)=1$.

由欧拉定理，$a^x \equiv a^{x+\varphi(n)} \pmod{n}$. 因此只需枚举 $0 \leqslant x < \varphi(n)$.
分块优化. 设 $x = p\left\lceil \sqrt{\varphi(n)} \right\rceil - q$，这里 $0 < p,q \leqslant \left\lceil \sqrt{\varphi(n)} \right\rceil$.
则 $a^{p\lceil \sqrt{\varphi(n)} \rceil - q} \equiv b \pmod{n}$ 等价于 $a^{p\lceil \sqrt{\varphi(n)} \rceil} \equiv b \cdot a^q \pmod{n}$.
枚举 $0 < q \leqslant \left\lceil \sqrt{\varphi(n)} \right\rceil$，用 hash 表记录余数与 q 值的关系.
再枚举 p，找到使 x 最小的 p,q.
以上算法也被称为大步小步法 (BSGS).

1 因数与倍数

2 欧拉函数

3 三分法

- 例 6. [BZOJ1857] 传送带

1. 因数与倍数
2. 欧拉函数
3. 三分法
   - 例 6. [BZOJ1857] 传送带

例 6. [BZOJ1857] 传送带

在二维平面上有两个线段型传送带 AB 和 CD, 小明在传送带 AB 上的速度为 P, 在传送带 CD 上的速度为 Q, 在平面其余位置的速度为 R, 求小明从 A 走到 B 需要的最短时间.

例 6. [BZOJ1857] 传送带

在二维平面上有两个线段型传送带 AB 和 CD，小明在传送带 AB 上的速度为 P，在传送带 CD 上的速度为 Q，在平面其余位置的速度为 R，求小明从 A 走到 B 需要的最短时间.

$1 \leqslant P, Q, R \leqslant 10$，各点坐标 $\leqslant 1,000$.

例 6. [BZOJ1857] 传送带

在二维平面上有两个线段型传送带 AB 和 CD, 小明在传送带 AB 上的速度为 P, 在传送带 CD 上的速度为 Q, 在平面其余位置的速度为 R, 求小明从 A 走到 B 需要的最短时间.

$1 \leqslant P, Q, R \leqslant 10$, 各点坐标 $\leqslant 1,000$.

三分套三分.

谢谢大家

谢谢大家.