數論

王迪

北京大學
wayne.wangdi@pku.edu.cn

2015 年 2 月 1 日

素數

Definition

設 p 是大於 1 的整數，如果 p 的正整數因子只有 1 和 p，則稱 p 爲**素數**。

素數

Definition

設 p 是大於 1 的整數,如果 p 的正整數因子只有 1 和 p,則稱 p 為**素數**。

Theorem

素數有無限多個。

Definition

設 p 是大於 1 的整數,如果 p 的正整數因子只有 1 和 p,則稱 p 爲**素數**。

Theorem

素數有無限多個。

Theorem

以 $\pi(n)$ 表示不超過 n 的素數的個數,則

$$\lim_{n\to\infty} \frac{\pi(n)}{\frac{n}{\ln n}} = 1$$

Definition

設 p 是大於 1 的整數,如果 p 的正整數因子只有 1 和 p,則稱 p 爲**素數**。

Theorem

素數有無限多個。

Theorem

以 $\pi(n)$ 表示不超過 n 的素數的個數,則

$$\lim_{n\to\infty} \frac{\pi(n)}{\frac{n}{\ln n}} = 1$$

Example

給一個正整數 n,求與它距離最近的素數。

Example

給一個正整數 n,判斷它是否爲素數。

Example

給一個正整數 n,判斷它是否爲素數。

Solution

枚舉 2 到 $n-1$ 的整數,判斷整除性。時間複雜度 $O(n)$。

Example

給一個正整數 n,判斷它是否爲素數。

Solution

枚舉 2 到 $n-1$ 的整數,判斷整除性。時間複雜度 $O(n)$。

Solution

枚舉 2 到 $\lfloor\sqrt{n}\rfloor$ 的整數,判斷整除性。時間複雜度 $O(\sqrt{n})$。

Example

給一個正整數 n,判斷它是否爲素數。

Solution

枚舉 2 到 $n-1$ 的整數,判斷整除性。時間複雜度 $O(n)$。

Solution

枚舉 2 到 $\lfloor\sqrt{n}\rfloor$ 的整數,判斷整除性。時間複雜度 $O(\sqrt{n})$。

嚴格意義上來講這兩個算法的複雜度都是指數級的。

Theorem (費馬小定理)

設 p 是一個素數, a 是一個整數且不是 p 的倍數, 那麼

$$a^{p-1} \equiv 1 \pmod{p}$$

Theorem (費馬小定理)

設 p 是一個素數, a 是一個整數且不是 p 的倍數, 那麼

$$a^{p-1} \equiv 1 \pmod{p}$$

Proof.

注意到若有 $i \not\equiv j \pmod{p}$, 那麼有 $i \times a \not\equiv j \times a \pmod{p}$。所以有

$$1 \times 2 \times 3 \times \cdots \times (p-1) \equiv (1 \times a) \times (2 \times a) \times \cdots \times ((p-1) \times a) \pmod{p}$$

即

$$W \equiv W \times a^{p-1} \pmod{p}$$

這裏 $W = 1 \times 2 \times 3 \times \cdots \times (p-1)$, 又 $(W, p) = 1$, 故

$$a^{p-1} \equiv 1 \pmod{p}$$

$\square$

費馬小定理的逆定理並不成立。

費馬小定理的逆定理並不成立。

對 $a = 2$,有 $n = 341$,滿足 $2^{n-1} \bmod n = 1$,但 $n = 11 \times 31$。

費馬小定理的逆定理並不成立。

對 $a=2$,有 $n=341$,滿足 $2^{n-1} \bmod n = 1$,但 $n = 11 \times 31$。

Definition

對於整數 a,稱滿足 $a^{n-1} \bmod n = 1$ 的合數爲以 a 爲底的**僞素數**。

費馬小定理的逆定理並不成立。

對 $a = 2$,有 $n = 341$,滿足 $2^{n-1} \bmod n = 1$,但 $n = 11 \times 31$。

Definition

對於整數 a,稱滿足 $a^{n-1} \bmod n = 1$ 的合數爲以 a 爲底的**僞素數**。

前 10 億的自然數中,同時以 2 和 3 爲底的僞素數有 1272 個。

費馬小定理的逆定理並不成立。

對 $a = 2$,有 $n = 341$,滿足 $2^{n-1} \bmod n = 1$,但 $n = 11 \times 31$。

Definition

對於整數 a,稱滿足 $a^{n-1} \bmod n = 1$ 的合數爲以 a 爲底的**僞素數**。

前 10 億的自然數中,同時以 2 和 3 爲底的僞素數有 1272 個。

Solution

隨機選取若干個小於待測整數的正整數作爲底 a,然後用費馬小定理來測試。

費馬小定理的逆定理並不成立。

對 $a = 2$,有 $n = 341$,滿足 $2^{n-1} \bmod n = 1$,但 $n = 11 \times 31$。

Definition

對於整數 a,稱滿足 $a^{n-1} \bmod n = 1$ 的合數爲以 a 爲底的**僞素數**。

前 10 億的自然數中,同時以 2 和 3 爲底的僞素數有 1272 個。

Solution

隨機選取若干個小於待測整數的正整數作爲底 a,然後用費馬小定理來測試。

但是,有些**坑爹**的合數能通過所有的測試!

如有興趣請自行搜索 Carmichael 數。

歷史上有一對好基友,他們叫做 Miller 和 Rabin。

歷史上有一對好基友,他們叫做 Miller 和 Rabin。

Theorem

若 p 是素數,x 是一個整數,且 $x^2 \bmod p = 1$,那麼 $x \equiv \pm 1 \pmod{p}$。

歷史上有一對好基友,他們叫做 Miller 和 Rabin。

Theorem

若 p 是素數,x 是一個整數,且 $x^2 \bmod p = 1$,那麼 $x \equiv \pm 1 \pmod{p}$。

Proof.

由 $x^2 \bmod p = 1$ 即 $p | x^2 - 1$ 即 $p | (x+1)(x-1)$,由 p 是素數易證。 □

歷史上有一對好基友,他們叫做 Miller 和 Rabin。

Theorem

若 p 是素數,x 是一個整數,且 $x^2 \bmod p = 1$,那麼 $x \equiv \pm 1 \pmod{p}$。

Proof.

由 $x^2 \bmod p = 1$ 即 $p | x^2 - 1$ 即 $p | (x+1)(x-1)$,由 p 是素數易證。 □

Corollary

設待測數爲 n,取一個比 n 小的正整數 a,設 $n - 1 = d \times 2^r$,若 n 是素數,則要麼 $a^d \bmod n = 1$,要麼存在一個 i,滿足 $0 \le i < r$ 且 $a^{d \times 2^i} \bmod n = -1$。

歷史上有一對好基友,他們叫做 Miller 和 Rabin。

Theorem

若 p 是素數,x 是一個整數,且 $x^2 \bmod p = 1$,那麼 $x \equiv \pm 1 \pmod{p}$。

Proof.

由 $x^2 \bmod p = 1$ 即 $p | x^2 - 1$ 即 $p | (x+1)(x-1)$,由 p 是素數易證。 □

Corollary

設待測數爲 n,取一個比 n 小的正整數 a,設 $n - 1 = d \times 2^r$,若 n 是素數,則要麼 $a^d \bmod n = 1$,要麼存在一個 i,滿足 $0 \le i < r$ 且 $a^{d \times 2^i} \bmod n = -1$。

Solution (Miller-Rabin)

隨機選取 k 個小於待測數 n 的正整數作爲底 a,用上述推論的逆定理來測試。
時間複雜度 $O(k \log n)$。

歷史上有一對好基友,他們叫做 Miller 和 Rabin。

Theorem

若 p 是素數,x 是一個整數,且 $x^2 \bmod p = 1$,那麼 $x \equiv \pm 1 \pmod{p}$。

Proof.

由 $x^2 \bmod p = 1$ 即 $p | x^2 - 1$ 即 $p | (x+1)(x-1)$,由 p 是素數易證。 □

Corollary

設待測數爲 n,取一個比 n 小的正整數 a,設 $n - 1 = d \times 2^r$,若 n 是素數,則要麼 $a^d \bmod n = 1$,要麼存在一個 i,滿足 $0 \le i < r$ 且 $a^{d \times 2^i} \bmod n = -1$。

Solution (Miller-Rabin)

隨機選取 k 個小於待測數 n 的正整數作爲底 a,用上述推論的逆定理來測試。

時間複雜度 $O(k \log n)$。

這種方法仍能找到反例,但以 2 和 3 爲底時,第一個反例就大到了 1373653。

Example

給一個正整數 n,求出不超過 n 的所有素數。

Example

給一個正整數 n,求出不超過 n 的所有素數。

Solution

枚舉 1 到 n 的數做素數測試,時間複雜度 $O(n \log n)$。

Example

給一個正整數 n,求出不超過 n 的所有素數。

Solution

枚舉 1 到 n 的數做素數測試,時間複雜度 $O(n \log n)$。

注意到這樣沒有利用數據範圍是 $[1, n]$ 這個條件。

Example

給一個正整數 n,求出不超過 n 的所有素數。

Solution

枚舉 1 到 n 的數做素數測試,時間複雜度 $O(n \log n)$。

注意到這樣沒有利用數據範圍是 $[1, n]$ 這個條件。

Solution

逐次枚舉 2 到 n,設當前枚舉到 x,那麼對所有滿足 $1 < k \leq \lfloor \frac{n}{x} \rfloor$ 的 k,把 $k \times x$ 標記爲「非素數」。時間複雜度 $O(n \log n)$。

Example

給一個正整數 n,求出不超過 n 的所有素數。

Solution

枚舉 1 到 n 的數做素數測試,時間複雜度 $O(n \log n)$。

注意到這樣沒有利用數據範圍是 $[1, n]$ 這個條件。

Solution

逐次枚舉 2 到 n,設當前枚舉到 x,那麼對所有滿足 $1 < k \leq \lfloor \frac{n}{x} \rfloor$ 的 k,把 $k \times x$ 標記爲「非素數」。時間複雜度 $O(n \log n)$。

篩法!

素數

Solution (線性篩法)

```
for (int i = 2; i <= n; ++ i) {
  if (!not_prime[i]) prime[++ prime_cnt] = i;
  for (int j = 1; j <= prime_cnt; ++ j) {
    if (prime[j] * i > n) break;
    not_prime[prime[j] * i] = true;
    if (i % prime[j] == 0) break;
  }
}
```

素數

Solution (線性篩法)

```
for (int i = 2; i <= n; ++ i) {
  if (!not_prime[i]) prime[++ prime_cnt] = i;
  for (int j = 1; j <= prime_cnt; ++ j) {
    if (prime[j] * i > n) break;
    not_prime[prime[j] * i] = true;
    if (i % prime[j] == 0) break;
  }
}
```

Solution (線性篩法)

該算法保證了每個合數都只會被自己**最小**的素因子篩去。

最大公約數

Definition (最大公約數)

$$(a, b) = \max\{d : d|a \text{ and } d|b\}$$

最大公約數

Definition (最大公約數)

$(a, b) = \max\{d : d|a \text{ and } d|b\}$

Definition (最小公倍數)

$[a, b] = \min\{m : a|m \text{ and } b|m\}$

最大公約數

Definition (最大公約數)

$(a, b) = \max\{d : d|a \text{ and } d|b\}$

Definition (最小公倍數)

$[a, b] = \min\{m : a|m \text{ and } b|m\}$

Example

給兩個整數 a 和 b,求它們的最大公約數。

最大公約數

Definition (最大公約數)

$(a, b) = \max\{d : d|a \text{ and } d|b\}$

Definition (最小公倍數)

$[a, b] = \min\{m : a|m \text{ and } b|m\}$

Example

給兩個整數 a 和 b,求它們的最大公約數。

Solution (歐幾里得算法)

```
int gcd(int a, int b) {
  if (b == 0) return a;
  else return gcd(b, a % b);
}
```

Definition (最大公約數)

$(a, b) = \max\{d : d|a \text{ and } d|b\}$

Definition (最小公倍數)

$[a, b] = \min\{m : a|m \text{ and } b|m\}$

Example

給兩個整數 a 和 b,求它們的最大公約數。

Solution (歐幾里得算法)

```
int gcd(int a, int b) {
  if (b == 0) return a;
  else return gcd(b, a % b);
}
```

求 n 個不超過 m 的正整數的最大公約數的複雜度是 $O(n + \log m)$。

Example

求不定方程 $ax + by = m$ 的整數解。

Example

求不定方程 $ax+by=m$ 的整數解。

Theorem

$ax+by=m$ 有整數解當且僅當 $(a,b)|m$。

Example

求不定方程 $ax + by = m$ 的整數解。

Theorem

$ax + by = m$ 有整數解當且僅當 $(a, b)|m$。

Theorem

設 (x_0, y_0) 是不定方程 $ax + by = m$ 的一組解，$(a, b) = g$，那麼解集爲

$$\{(x_0 + \frac{b}{g}t, y_0 - \frac{a}{g}t) : t \in \mathbb{Z}\}$$

最大公約數

Solution (擴展歐幾里得算法)

```
int ext_gcd(int a, int b, int &x, int &y) {
  if (b == 0) {
    x = 1, y = 0;
    return a;
  }
  else {
    int g = ext_gcd(b, a % b, x, y);
    int t = x;
    x = y, y = t - a / b * x;
    return g;
  }
}
```

最大公約數

Solution (擴展歐幾里得算法)

```
int ext_gcd(int a, int b, int &x, int &y) {
  if (b == 0) {
    x = 1, y = 0;
    return a;
  }
  else {
    int g = ext_gcd(b, a % b, x, y);
    int t = x;
    x = y, y = t - a / b * x;
    return g;
  }
}
```

考慮從 $bx + (a \bmod b)y = g$ 的 (x, y) 推導到 $ax' + by' = g$ 的 (x', y')。

Example

求解線性同餘方程組

$$x \equiv b_1 \pmod{m_1}$$
$$x \equiv b_2 \pmod{m_2}$$
$$\cdots$$
$$x \equiv b_k \pmod{m_k}$$

Example

求解線性同餘方程組

$$x \equiv b_1 \pmod{m_1}$$
$$x \equiv b_2 \pmod{m_2}$$
$$\cdots$$
$$x \equiv b_k \pmod{m_k}$$

Solution

當 m_i 兩兩互素時,可以用經典的中國剩餘定理。

Example

求解線性同餘方程組

$$x \equiv b_1 \pmod{m_1}$$
$$x \equiv b_2 \pmod{m_2}$$
$$\cdots$$
$$x \equiv b_k \pmod{m_k}$$

Solution

當 m_i 兩兩互素時,可以用經典的中國剩餘定理。

Solution

介紹一種基於「合併」思想的算法,當 m_i 不滿足兩兩互素時,也同樣能夠工作。

Solution

$$x \equiv b_1 \pmod{m_1}$$

$$x \equiv b_2 \pmod{m_2}$$

Solution

$$x \equiv b_1 \pmod{m_1}$$

$$x \equiv b_2 \pmod{m_2}$$

可以寫成

$$x = k_1 m_1 + b_1$$

$$x = k_2 m_2 + b_2$$

$$k_1 m_1 - k_2 m_2 = b_2 - b_1$$

Solution

$$x \equiv b_1 \pmod{m_1}$$
$$x \equiv b_2 \pmod{m_2}$$

可以寫成

$$x = k_1 m_1 + b_1$$
$$x = k_2 m_2 + b_2$$
$$k_1 m_1 - k_2 m_2 = b_2 - b_1$$

設 $g = (m_1, m_2)$,若 $b_2 - b_1$ 能被 g 整除,則可以繼續

$$\frac{m_1}{g} k_1 \equiv \frac{b_2 - b_1}{g} \pmod{\frac{m_2}{g}}$$

Solution

$$x \equiv b_1 \pmod{m_1}$$

$$x \equiv b_2 \pmod{m_2}$$

可以寫成

$$x = k_1 m_1 + b_1$$

$$x = k_2 m_2 + b_2$$

$$k_1 m_1 - k_2 m_2 = b_2 - b_1$$

設 $g = (m_1, m_2)$,若 $b_2 - b_1$ 能被 g 整除,則可以繼續

$$\frac{m_1}{g} k_1 \equiv \frac{b_2 - b_1}{g} \pmod{\frac{m_2}{g}}$$

用擴展歐幾里得算法算出 $k_1 \equiv T \pmod{\frac{m_2}{g}}$,則兩個同餘式可以合併為

$$x \equiv T m_1 + b_1 \pmod{\frac{m_1 m_2}{g}}$$

Definition

設正整數 m,對於任意正整數 a 滿足 $(a, m) = 1$,總存在惟一的 b 滿足 $a \times b \equiv 1 \pmod{m}$ 且 $1 \leq b < m$,稱 b 爲模 m 意義下的**逆元**。

Definition

設正整數 m,對於任意正整數 a 滿足 $(a, m) = 1$,總存在惟一的 b 滿足 $a \times b \equiv 1 \pmod{m}$ 且 $1 \leq b < m$,稱 b 爲模 m 意義下的**逆元**。

Example

給出正整數 a 和 m,保證 $(a, m) = 1$,求模 m 意義下 a 的逆元。

Definition

設正整數 m,對於任意正整數 a 滿足 $(a, m) = 1$,總存在惟一的 b 滿足 $a \times b \equiv 1 \pmod{m}$ 且 $1 \le b < m$,稱 b 爲模 m 意義下的**逆元**。

Example

給出正整數 a 和 m,保證 $(a, m) = 1$,求模 m 意義下 a 的逆元。

Solution

根據定義,用擴展歐幾里得算法解一個線性同餘方程即可。

Definition

設正整數 m,對於任意正整數 a 滿足 $(a,m)=1$,總存在惟一的 b 滿足 $a \times b \equiv 1 \pmod{m}$ 且 $1 \leq b < m$,稱 b 爲模 m 意義下的**逆元**。

Example

給出正整數 a 和 m,保證 $(a,m)=1$,求模 m 意義下 a 的逆元。

Solution

根據定義,用擴展歐幾里得算法解一個線性同餘方程即可。

注意到 $a \times b \equiv 1 \pmod{m}$ 可以認爲是 $b \equiv \frac{1}{a} \pmod{m}$,所以當我們需要在模 m 意義下除以 a 時,可以用乘上 b 來實現,這就是逆元的用途。

Definition

定義在 $\mathbb{N}^*$ 上的函數 $f\colon \mathbb{N}^* \to A$ 都可以稱作是**數論函數**,其中 A 可以是有加減乘運算的任意集合。

Definition

定義在 $\mathbb{N}^*$ 上的函數 $f\colon \mathbb{N}^* \to A$ 都可以稱作是**數論函數**,其中 A 可以是有加減乘運算的任意集合。

一些常見的數論函數:

- $\sigma(n) = \sum_{d|n} d$,表示正整數 n 的正因子之和。
- $\tau(n) = \sum_{d|n} 1$,表示正整數 n 的正因子個數。

Definition

定義在 $\mathbb{N}^*$ 上的函數 $f\colon \mathbb{N}^* \to A$ 都可以稱作是**數論函數**,其中 A 可以是有加減乘運算的任意集合。

一些常見的數論函數:

- $\sigma(n) = \sum_{d|n} d$,表示正整數 n 的正因子之和。
- $\tau(n) = \sum_{d|n} 1$,表示正整數 n 的正因子個數。

Definition

數論函數 f 叫做是**積性函數**,如果對於任意兩個互素的正整數 n 和 m,都滿足 $f(nm) = f(n)f(m)$。

Definition

定義在 $\mathbb{N}^*$ 上的函數 $f\colon \mathbb{N}^* \to A$ 都可以稱作是**數論函數**,其中 A 可以是有加減乘運算的任意集合。

一些常見的數論函數:

- $\sigma(n) = \sum_{d|n} d$,表示正整數 n 的正因子之和。
- $\tau(n) = \sum_{d|n} 1$,表示正整數 n 的正因子個數。

Definition

數論函數 f 叫做是**積性函數**,如果對於任意兩個互素的正整數 n 和 m,都滿足 $f(nm) = f(n)f(m)$。

Corollary

若 $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$,則有

$$f(n) = f(p_1^{a_1})f(p_2^{a_2}) \cdots f(p_k^{a_k}) = \prod_{i=1}^{k} f(p_i^{a_i})$$

Definition (卷積)

對於數論函數 f 和 g,它們的卷積表示成 $f * g$,卷積的結果是一個數論函數 h,且

$$h(n) = \sum_{d|n} f(d) g(\frac{n}{d})$$

Definition (卷積)

對於數論函數 f 和 g,它們的卷積表示成 $f * g$,卷積的結果是一個數論函數 h,且

$$h(n) = \sum_{d|n} f(d)g(\frac{n}{d})$$

Theorem

數論函數的卷積滿足交換律和結合律。

Definition (卷積)

對於數論函數 f 和 g,它們的卷積表示成 $f*g$,卷積的結果是一個數論函數 h,且

$$h(n)=\sum_{d|n}f(d)g(\frac{n}{d})$$

Theorem

數論函數的卷積滿足交換律和結合律。

思考題:證明結合律。

引入另外一個很重要的數論函數 μ,其中 $\mu(1) = 1$,而對 $n \geq 2$ 時

- 若 n 是 r 個不同的素數之積,則 $\mu(n) = (-1)^r$。
- 否則,$\mu(n) = 0$。

引入另外一個很重要的數論函數 μ,其中 $\mu(1)=1$,而對 $n\geq 2$ 時

- 若 n 是 r 個不同的素數之積,則 $\mu(n)=(-1)^r$。
- 否則,$\mu(n)=0$。

這個數論函數 μ 叫做**莫比烏斯函數**。

引入另外一個很重要的數論函數 μ,其中 $\mu(1)=1$,而對 $n\geq 2$ 時

- 若 n 是 r 個不同的素數之積,則 $\mu(n)=(-1)^r$。
- 否則,$\mu(n)=0$。

這個數論函數 μ 叫做**莫比烏斯函數**。

Corollary

μ 是積性函數。

引入另外一個很重要的數論函數 μ,其中 $\mu(1) = 1$,而對 $n \geq 2$ 時

- 若 n 是 r 個不同的素數之積,則 $\mu(n) = (-1)^r$。
- 否則,$\mu(n) = 0$。

這個數論函數 μ 叫做**莫比烏斯函數**。

Corollary

μ 是積性函數。

Corollary

$\sum_{d|n} \mu(d) = [n = 1]$,其中 $[cond]$ 表示 $cond$ 這個條件是否成立。

Theorem (莫比烏斯反演公式)

設兩個數論函數 f 和 g,則下面兩個命題是彼此等價的

- 對每個正整數 $n, f(n) = \sum_{d|n} g(d)$。
- 對每個正整數 $n, g(n) = \sum_{d|n} \mu(d) f(\frac{n}{d})$。

Theorem (莫比烏斯反演公式)

設兩個數論函數 f 和 g,則下面兩個命題是彼此等價的

- 對每個正整數 $n, f(n) = \sum_{d|n} g(d)$。
- 對每個正整數 $n, g(n) = \sum_{d|n} \mu(d) f(\frac{n}{d})$。

Proof.

定義數論函數 $e, e(1) = 1$,當 $n \geq 2$ 時 $e(n) = 0$。再用 $\{1\}$ 來表示一個值恆爲 1 的數論函數。

易證對任意數論函數 f,有 $f * e = f$。另外還有 $\mu * \{1\} = e$。

則需要證明的式子可寫成:$f = g * \{1\}, g = f * \mu$。然後:

- $f * \mu = (g * \{1\}) * \mu = g * (\{1\} * \mu) = g * e = g$
- $g * \{1\} = (f * \mu) * \{1\} = f * (\mu * \{1\}) = f * e = f$

$\square$

Definition

對每個正整數 n,以 $\varphi(n)$ 表示 1 到 n 中與 n 互素的數的個數,稱作**歐拉函數**。

Definition

對每個正整數 n,以 $\varphi(n)$ 表示 1 到 n 中與 n 互素的數的個數,稱作**歐拉函數**。

Theorem

φ 是積性函數。

Definition

對每個正整數 n,以 $\varphi(n)$ 表示 1 到 n 中與 n 互素的數的個數,稱作**歐拉函數**。

Theorem

φ 是積性函數。

Theorem

設 $n \geq 2, n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ 是正整數 n 的標準分解式,則

$$\varphi(n) = \prod_{k=1}^{n} (p_i^{a_i} - p_i^{a_i - 1}) = n \prod_{i=1}^{k} (1 - \frac{1}{p_i})$$

Corollary

$\sum_{d|n}\varphi(d) = n$。

Corollary

$\sum_{d|n} \varphi(d) = n$。

Proof.

$$\varphi(n) \quad = \sum_{i=1}^{n} [(i, n) = 1]$$

Corollary

$\sum_{d|n}\varphi(d)=n$。

Proof.

$$
\begin{aligned}
\varphi(n) &= \sum_{i=1}^{n}[(i,n)=1] \\
&= \sum_{i=1}^{n}\sum_{d|(i,n)}\mu(d)
\end{aligned}
$$

Corollary

$\sum_{d|n} \varphi(d) = n$。

Proof.

$$\begin{aligned}\varphi(n) &= \sum_{i=1}^{n}[(i,n)=1] \\ &= \sum_{i=1}^{n}\sum_{d|(i,n)}\mu(d) \\ &= \sum_{d|n}\mu(d)(\frac{n}{d})\end{aligned}$$

Corollary

$\sum_{d|n} \varphi(d) = n$。

Proof.

$$\begin{aligned}\varphi(n) &= \sum_{i=1}^{n} [(i, n) = 1] \\ &= \sum_{i=1}^{n} \sum_{d|(i,n)} \mu(d) \\ &= \sum_{d|n} \mu(d)(\frac{n}{d})\end{aligned}$$

設 $f(n) = n$,則 $\varphi(n) = \sum_{d|n} \mu(d) f(\frac{n}{d})$,由莫比烏斯反演得 $f(n) = \sum_{d|n} \varphi(d)$。 $\square$

記住這兩個重要的結論：

- $\sum_{d|n} \mu(d) = [n = 1]$
- $\sum_{d|n} \varphi(d) = n$

記住這兩個重要的結論：

- $\sum_{d|n} \mu(d) = [n = 1]$
- $\sum_{d|n} \varphi(d) = n$

Example

給出一個正整數 n，預處理出 1 到 n 的 μ、φ、σ、τ 函數的值。

記住這兩個重要的結論:

- $\sum_{d|n} \mu(d) = [n = 1]$
- $\sum_{d|n} \varphi(d) = n$

Example

給出一個正整數 n,預處理出 1 到 n 的 μ、φ、σ、τ 函數的值。

Solution

利用積性函數的性質,又由線性篩法可以找到每個數的最小素因子的特質,這些函數值均可 $O(n)$ 時間預處理。

Example

給出兩個正整數 n 和 $m(n \leq m)$，求 $\sum_{i=1}^{n} \sum_{j=1}^{m} (i, j)$。

Example

給出兩個正整數 n 和 $m(n \leq m)$，求 $\sum_{i=1}^{n} \sum_{j=1}^{m} (i, j)$。

Solution

$$\sum_{i=1}^{n} \sum_{j=1}^{m} (i, j) = \sum_{i=1}^{n} \sum_{j=1}^{m} \sum_{d \mid (i,j)} \varphi(d)$$

Example

給出兩個正整數 n 和 $m(n \leq m)$，求 $\sum_{i=1}^{n} \sum_{j=1}^{m} (i,j)$。

Solution

$$\begin{aligned}\textstyle\sum_{i=1}^{n} \sum_{j=1}^{m} (i,j) &= \sum_{i=1}^{n} \sum_{j=1}^{m} \sum_{d|(i,j)} \varphi(d) \\ &= \sum_{i=1}^{n} \sum_{j=1}^{m} \sum_{d|i \ and \ d|j} \varphi(d)\end{aligned}$$

Example

給出兩個正整數 n 和 $m(n \leq m)$，求 $\sum_{i=1}^{n}\sum_{j=1}^{m}(i,j)$。

Solution

$$
\begin{aligned}
\sum_{i=1}^{n}\sum_{j=1}^{m}(i,j) &= \sum_{i=1}^{n}\sum_{j=1}^{m}\sum_{d|(i,j)}\varphi(d)\\
&= \sum_{i=1}^{n}\sum_{j=1}^{m}\sum_{d|i \ and \ d|j}\varphi(d)\\
&= \sum_{d=1}^{n}\varphi(d)\lfloor\frac{n}{d}\rfloor\lfloor\frac{m}{d}\rfloor
\end{aligned}
$$

Example

給出兩個正整數 n 和 $m(n \leq m)$，求 $\sum_{i=1}^{n} \sum_{j=1}^{m} (i,j)$。

Solution

$$\begin{aligned}
\sum_{i=1}^{n} \sum_{j=1}^{m} (i,j) &= \sum_{i=1}^{n} \sum_{j=1}^{m} \sum_{d|(i,j)} \varphi(d) \\
&= \sum_{i=1}^{n} \sum_{j=1}^{m} \sum_{d|i \ and \ d|j} \varphi(d) \\
&= \sum_{d=1}^{n} \varphi(d) \lfloor \frac{n}{d} \rfloor \lfloor \frac{m}{d} \rfloor
\end{aligned}$$

一個事實是:$\lfloor \frac{x}{i} \rfloor$ 的不同的取值個數是 $O(\sqrt{x})$ 的。與是利用線性篩法預處理 φ 的前綴和,就可以做到單組詢問 $O(\sqrt{n})$ 了。

Example

求 $\sum_{i=1}^{n}\sum_{j=1}^{m}[(i,j)=1]$。

Example

求 $\sum_{i=1}^{n}\sum_{j=1}^{m}[(i,j)=1]$。

Solution

做法與上題一樣，不過是把 φ 換成 μ。

數論函數

Example

求 $\sum_{i=1}^{n}\sum_{j=1}^{m}[(i,j)=1]$。

Solution

做法與上題一樣，不過是把 φ 換成 μ。

代碼小技巧：

```
for (int i = 1; i <= n; ) {
  int j = n / (n / i);
  res += (phi_sum[j] - phi_sum[i - 1]) * (n / i);
  i = j + 1;
}
```

Theorem (費馬小定理)

設 p 是一個素數, a 是一個整數且不是 p 的倍數, 那麼

$$a^{p-1} \equiv 1 \pmod p$$

Theorem (費馬小定理)

設 p 是一個素數, a 是一個整數且不是 p 的倍數,那麼

$$a^{p-1} \equiv 1 \pmod{p}$$

Theorem (歐拉定理)

設 m 爲正整數, a 是與 m 互素的整數,則

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

Theorem (費馬小定理)

設 p 是一個素數,a 是一個整數且不是 p 的倍數,那麼

$$a^{p-1} \equiv 1 \pmod{p}$$

Theorem (歐拉定理)

設 m 爲正整數,a 是與 m 互素的整數,則

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

顯然,費馬小定理是歐拉定理的特例。歐拉定理的證明則與費馬小定理的證明相似,只需取與 m 互素的 $\varphi(m)$ 個數就行了。

Theorem (費馬小定理)

設 p 是一個素數,a 是一個整數且不是 p 的倍數,那麼

$$a^{p-1} \equiv 1 \pmod{p}$$

Theorem (歐拉定理)

設 m 爲正整數,a 是與 m 互素的整數,則

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

顯然,費馬小定理是歐拉定理的特例。歐拉定理的證明則與費馬小定理的證明相似,只需取與 m 互素的 $\varphi(m)$ 個數就行了。

Corollary

設 m 爲正整數,$x \geq \varphi(m)$,則

$$a^x \equiv a^{x \bmod \varphi(m)+\varphi(m)} \pmod{m}$$

Definition

設 $(a, m) = 1$,滿足 $a^r \equiv 1 \pmod{m}$ 的最小正整數 r 叫做整數 a 模 m 的**階**。

原根

Definition

設 $(a, m) = 1$,滿足 $a^r \equiv 1 \pmod{m}$ 的最小正整數 r 叫做整數 a 模 m 的**階**。

Theorem

設 $(a, m) = 1$,r 爲 a 模 m 的階,則對每個正整數 k,$a^k \equiv 1 \pmod{m}$ 當且僅當 $r|k$。特別地,$r|\varphi(m)$。

Definition

設 $(a, m) = 1$,滿足 $a^r \equiv 1 \pmod{m}$ 的最小正整數 r 叫做整數 a 模 m 的**階**。

Theorem

設 $(a, m) = 1$,r 爲 a 模 m 的階,則對每個正整數 k,$a^k \equiv 1 \pmod{m}$ 當且僅當 $r|k$。特別地,$r|\varphi(m)$。

Proof.

設 $k = qr + s$,其中 $0 \le s < r$。由 $a^k \equiv 1 \equiv a^r \pmod{m}$ 和 $(a, m) = 1$ 可知

$$a^s \equiv a^{k-qr} \equiv a^k \cdot (a^r)^{-q} \equiv 1 \pmod{m}$$

但是 r 是滿足 $a^x \equiv 1 \pmod{m}$ 的最小正整數,而 $0 \le s < r$,故 $s = 0$。 $\square$

Corollary

設 $(a, m) = 1$,則 a 模 m 的階是 r,當且僅當下列二條件成立:

- $a^r \equiv 1 \pmod{m}$。
- 對於 r 的每個素因子 p 有 $a^{\frac{r}{p}} \not\equiv 1 \pmod{m}$。

Corollary

設 $(a, m) = 1$,則 a 模 m 的階是 r,當且僅當下列二條件成立:

- $a^r \equiv 1 \pmod{m}$。
- 對於 r 的每個素因子 p 有 $a^{\frac{r}{p}} \not\equiv 1 \pmod{m}$。

Proof.

若 a 模 m 的階是 r,那麼這兩個條件顯然成立。反之,設 l 爲 a 模 m 的階,由第一個條件知 $l | r$,若 $l \neq r$,則 $s = \frac{r}{l} > 1$,所以 s 有素因子 p,即 $s = pt$,與是 $\frac{r}{p} = lt$,而 $a^{\frac{r}{p}} = (a^l)^t \equiv 1 \pmod{m}$,這就和第二個條件矛盾了。 $\square$

原根

Definition

若整數 a 模 m 的階爲 $\varphi(m)$,則 a 叫做是模 m 的**原根**。

Definition

若整數 a 模 m 的階爲 $\varphi(m)$,則 a 叫做是模 m 的**原根**。

Theorem

對於正整數 m,模 m 具有原根當且僅當 $m = 2, 4, p^a, 2p^a$,其中 p 是奇素數且 $a \geq 1$。

原根

Definition

若整數 a 模 m 的階爲 $\varphi(m)$,則 a 叫做是模 m 的**原根**。

Theorem

對於正整數 m,模 m 具有原根當且僅當 $m = 2, 4, p^a, 2p^a$,其中 p 是奇素數且 $a \geq 1$。

Example

給出一個具有原根的模 m,找出任意一個原根。

原根

Definition

若整數 a 模 m 的階爲 $\varphi(m)$,則 a 叫做是模 m 的**原根**。

Theorem

對於正整數 m,模 m 具有原根當且僅當 $m = 2, 4, p^a, 2p^a$,其中 p 是奇素數且 $a \geq 1$。

Example

給出一個具有原根的模 m,找出任意一個原根。

Solution

因爲原根通常都很小,所以從小往大枚舉,用之前的推論來判定即可。

原根

設模 m 有原根 g,則 $\{1, g, g^2, \cdots, g^{\varphi(m)-1}\}$ 爲模 m 的縮系。所以對每個與 m 互素的整數 a,必存在惟一的整數 k,使得

$$a \equiv g^k \pmod{m}, 0 \leq k \leq \varphi(m) - 1$$

設模 m 有原根 g,則 $\{1, g, g^2, \cdots, g^{\varphi(m)-1}\}$ 爲模 m 的縮系。所以對每個與 m 互素的整數 a,必存在惟一的整數 k,使得

$$a \equiv g^k \pmod m, 0 \le k \le \varphi(m) - 1$$

Definition

上述的 k 叫做 a(對於原根 g)模 m 的**指數**,表示成 $k = \mathrm{ind}_g a$。指數也叫做**離散對數**。

設模 m 有原根 g,則 $\{1, g, g^2, \cdots, g^{\varphi(m)-1}\}$ 爲模 m 的縮系。所以對每個與 m 互素的整數 a,必存在惟一的整數 k,使得

$$a \equiv g^k \pmod{m}, 0 \leq k \leq \varphi(m) - 1$$

Definition

上述的 k 叫做 a(對於原根 g)模 m 的**指數**,表示成 $k = \mathrm{ind}_g a$。指數也叫做**離散對數**。

Theorem

設 $(a, m) = (b, m) = 1$,則

- $a \equiv b \pmod{m}$ 當且僅當 $ind_g a = ind_g b$。
- $ind_g ab \equiv ind_g a + ind_g b \pmod{\varphi(m)}$。
- $ind_g a^n \equiv n \cdot ind_g a \pmod{\varphi(m)}$,$n$ 是整數。

Example

給出同餘方程 $a^x \equiv b \pmod{m}$,保證 $(a,m)=(b,m)=1$ 且模 m 具有原根,求 x 的最小整數解。

Example

給出同餘方程 $a^x \equiv b \pmod{m}$,保證 $(a,m)=(b,m)=1$ 且模 m 具有原根,求 x 的最小整數解。

Solution

找到 m 的一個原根 g,從 0 到 $\varphi(m)-1$ 枚舉 x 進行判定,時間複雜度 $O(\varphi(m))$。

Example

給出同餘方程 $a^x \equiv b \pmod{m}$，保證 $(a, m) = (b, m) = 1$ 且模 m 具有原根，求 x 的最小整數解。

Solution

找到 m 的一個原根 g，從 0 到 $\varphi(m) - 1$ 枚舉 x 進行判定，時間複雜度 $O(\varphi(m))$。

Solution

因爲 $0 \leq x \leq \varphi(m) - 1$，所以設 $t = \lfloor \sqrt{\varphi(m) - 1} \rfloor + 1$。

設 $x = pt + s$，其中 $0 \leq s < t$。我們枚舉 p 的所有可能的值，並用哈希表等數據結構存儲 $a^{pt} \bmod m$。

由 $(a, m) = (b, m) = 1$ 有 $a^{pt} \equiv a^{-s} b \pmod{m}$，所以再枚舉 s 的可能值，在數據結構中查詢 $a^{-s} b$ 即可。若不考慮數據結構的複雜度，時間複雜度爲 $O(\sqrt{\varphi(m)})$。

Example (SGU 261)

給出三個正整數 p, k, a,其中 p 是素數,保證有解,輸出所有滿足 $x^k \equiv a \pmod{p}$ 且 $0 \le x \le p-1$ 的整數 x。

Example (SGU 261)

給出三個正整數 p, k, a,其中 p 是素數,保證有解,輸出所有滿足 $x^k \equiv a \pmod{p}$ 且 $0 \le x \le p-1$ 的整數 x。

Solution

- 第一步,找出模 p 的一個原根 g。

Example (SGU 261)

給出三個正整數 p, k, a,其中 p 是素數,保證有解,輸出所有滿足 $x^k \equiv a \pmod{p}$ 且 $0 \le x \le p-1$ 的整數 x。

Solution

- 第一步,找出模 p 的一個原根 g。
- 第二步,求出 $ind_g a$,設爲 b,則有 $x^k \equiv g^b \pmod{p}$。

Example (SGU 261)

給出三個正整數 p, k, a,其中 p 是素數,保證有解,輸出所有滿足 $x^k \equiv a \pmod{p}$ 且 $0 \leq x \leq p-1$ 的整數 x。

Solution

- 第一步,找出模 p 的一個原根 g。
- 第二步,求出 $ind_g a$,設爲 b,則有 $x^k \equiv g^b \pmod{p}$。
- 第三步,對同餘式兩邊取離散對數有 $k \cdot ind_g x \equiv b \pmod{p-1}$。

Example (SGU 261)

給出三個正整數 p, k, a,其中 p 是素數,保證有解,輸出所有滿足 $x^k \equiv a \pmod{p}$ 且 $0 \le x \le p-1$ 的整數 x。

Solution

- 第一步,找出模 p 的一個原根 g。
- 第二步,求出 $ind_g a$,設爲 b,則有 $x^k \equiv g^b \pmod{p}$。
- 第三步,對同餘式兩邊取離散對數有 $k \cdot ind_g x \equiv b \pmod{p-1}$。
- 第四步,求解這個線性同餘方程,找出所有解。

Example

組合數的定義想必大家都是知道的：

$$C_m^n = \frac{n!}{m!(n-m)!}$$

給出非負整數 n、m 和正整數 k，求 $C_m^n \bmod k$。

Example

組合數的定義想必大家都是知道的:

$$C_m^n = \frac{n!}{m!(n-m)!}$$

給出非負整數 n、m 和正整數 k,求 $C_m^n \bmod k$。

Solution

先來一些簡單點的情況。

- $k = 1$,

Example

組合數的定義想必大家都是知道的:

$$C_m^n = \frac{n!}{m!(n-m)!}$$

給出非負整數 n、m 和正整數 k,求 $C_m^n \bmod k$。

Solution

先來一些簡單點的情況。

- $k = 1$,這種情況過於困難,不用管了。

Example

組合數的定義想必大家都是知道的:

$$C_m^n = \frac{n!}{m!(n-m)!}$$

給出非負整數 n、m 和正整數 k,求 $C_m^n \bmod k$。

Solution

先來一些簡單點的情況。

- $k = 1$,這種情況過於困難,不用管了。
- $k > 1$,

Example

組合數的定義想必大家都是知道的:

$$C_m^n = \frac{n!}{m!(n-m)!}$$

給出非負整數 n、m 和正整數 k,求 $C_m^n \bmod k$。

Solution

先來一些簡單點的情況。

- $k = 1$,這種情況過於困難,不用管了。
- $k > 1, 0 \le nm \le 10^7$。$O(nm)$ 遞推。

組合數求模

Example

組合數的定義想必大家都是知道的:

$$C_m^n = \frac{n!}{m!(n-m)!}$$

給出非負整數 n、m 和正整數 k,求 $C_m^n \bmod k$。

Solution

先來一些簡單點的情況。

- $k = 1$,這種情況過於困難,不用管了。
- $k > 1, 0 \le nm \le 10^7$。$O(nm)$ 遞推。
- $n \le 10^9, m \le 10^4, k \le 10^9$,

Example

組合數的定義想必大家都是知道的:

$$C_m^n = \frac{n!}{m!(n-m)!}$$

給出非負整數 n、m 和正整數 k,求 $C_m^n \bmod k$。

Solution

先來一些簡單點的情況。

- $k = 1$,這種情況過於困難,不用管了。
- $k > 1, 0 \le nm \le 10^7$。$O(nm)$ 遞推。
- $n \le 10^9, m \le 10^4, k \le 10^9$,由於 $C_m^n = \frac{n(n-1)(n-2)\cdots(n-m+1)}{m!}$,可以發現分子分母的項數都是可以接受的,這就又有兩種方法:

Example

組合數的定義想必大家都是知道的:

$$C_m^n = \frac{n!}{m!(n-m)!}$$

給出非負整數 n、m 和正整數 k,求 $C_m^n \bmod k$。

Solution

先來一些簡單點的情況。

- $k=1$,這種情況過於困難,不用管了。
- $k>1, 0 \le nm \le 10^7$。$O(nm)$ 遞推。
- $n \le 10^9, m \le 10^4, k \le 10^9$,由於 $C_m^n = \frac{n(n-1)(n-2)\cdots(n-m+1)}{m!}$,可以發現分子分母的項數都是可以接受的,這就又有兩種方法:
  - 對每個數字分解素因子,合併後用快速冪。

Example

組合數的定義想必大家都是知道的:

$$C_m^n = \frac{n!}{m!(n-m)!}$$

給出非負整數 n、m 和正整數 k,求 $C_m^n \bmod k$。

Solution

先來一些簡單點的情況。

- $k = 1$,這種情況過於困難,不用管了。
- $k > 1, 0 \le nm \le 10^7$。$O(nm)$ 遞推。
- $n \le 10^9, m \le 10^4, k \le 10^9$,由於 $C_m^n = \frac{n(n-1)(n-2)\cdots(n-m+1)}{m!}$,可以發現分子分母的項數都是可以接受的,這就又有兩種方法:
  - 對每個數字分解素因子,合併後用快速冪。
  - 對每個數字值分解 k 所含有的素因子,分母剩餘的部分用逆元解決。

Solution

然後我們稍微增加點難度。

Solution

然後我們稍微增加點難度。

- $n, m \leq 10^6, k \leq 10^9$,

組合數求模

Solution

然後我們稍微增加點難度。

- $n, m \leq 10^6, k \leq 10^9$, 對 $n!$ 分解素因子，大致複雜度是 $O(n)$。

Solution

然後我們稍微增加點難度。

- $n, m \leq 10^6, k \leq 10^9$,對 $n!$ 分解素因子,大致複雜度是 $O(n)$。
- $n, m \leq 10^{10}, k$ 是素數且較小,

Solution

然後我們稍微增加點難度。

- $n, m \leq 10^6, k \leq 10^9$,對 $n!$ 分解素因子,大致複雜度是 $O(n)$。
- $n, m \leq 10^{10}, k$ 是素數且較小,使用 $Lucas$ 定理。

Solution

然後我們稍微增加點難度。

- $n, m \leq 10^6, k \leq 10^9$,對 $n!$ 分解素因子,大致複雜度是 $O(n)$。
- $n, m \leq 10^{10}, k$ 是素數且較小,使用 *Lucas* 定理。

Theorem (Lucas 定理)

$$C_m^n \bmod p = \prod_{i=0}^{h} C_{m_i}^{n_i} \bmod p$$

這裏 n_i 和 m_i 表示把 n 和 m 分解爲 p 進制時第 i 位的值。

Solution

最後考慮這麼一種數據範圍，$n, m \leq 10^9$，$k \leq 10^5$。

Solution

最後考慮這麼一種數據範圍，$n, m \leq 10^9$，$k \leq 10^5$。

首先，我們可以利用中國剩餘定理，可以發現問題等價於求 $C_m^n \bmod p^c$，p 是素數，$c \geq 1$。

Solution

最後考慮這麼一種數據範圍，$n, m \le 10^9$，$k \le 10^5$。

首先，我們可以利用中國剩餘定理，可以發現問題等價於求 $C_m^n \bmod p^c$，p 是素數，$c \ge 1$。

我們考慮計算 $n!$，把中間的 p 都除開算出一個值，同時算出除開的 p 的個數。

Solution

最後考慮這麼一種數據範圍，$n, m \leq 10^9$，$k \leq 10^5$。

首先，我們可以利用中國剩餘定理，可以發現問題等價於求 $C_m^n \bmod p^c$，p 是素數，$c \geq 1$。

我們考慮計算 $n!$，把中間的 p 都除開算出一個值，同時算出除開的 p 的個數。

例如 $n = 19, p = 3, c = 2$，考慮 $19!$：

Solution

最後考慮這麼一種數據範圍，$n, m \leq 10^9$，$k \leq 10^5$。

首先，我們可以利用中國剩餘定理，可以發現問題等價於求 $C_m^n \bmod p^c$，p 是素數，$c \geq 1$。

我們考慮計算 $n!$，把中間的 p 都除開算出一個值，同時算出除開的 p 的個數。

例如 $n = 19, p = 3, c = 2$，考慮 $19!$：

$$19! = (1 \times 2 \times 4 \times 5 \times 7 \times \cdots \times 16 \times 17 \times 19) \times 3^6 \times (1 \times 2 \times 3 \times \cdots \times 6)$$

Solution

最後考慮這麼一種數據範圍，$n, m \le 10^9$，$k \le 10^5$。
首先，我們可以利用中國剩餘定理，可以發現問題等價於求 $C_m^n \bmod p^c$，p 是素數，$c \ge 1$。
我們考慮計算 $n!$，把中間的 p 都除開算出一個值，同時算出除開的 p 的個數。
例如 $n = 19, p = 3, c = 2$，考慮 $19!$：

$$19! = (1 \times 2 \times 4 \times 5 \times 7 \times \cdots \times 16 \times 17 \times 19) \times 3^6 \times (1 \times 2 \times 3 \times \cdots \times 6)$$

令 $f(n)$ 表示 $n!$ 中除去 p 因子後模 p^c 的值。若要求 $f(19)$，那麼就是上式的前半部分，然後 3^6 提出來，最後一部分對答案的貢獻是 $f(6)$，即 $f(\lfloor \frac{n}{p} \rfloor)$。對於前面，又有：

Solution

最後考慮這麼一種數據範圍，$n, m \le 10^9$，$k \le 10^5$。
首先，我們可以利用中國剩餘定理，可以發現問題等價於求 $C_m^n \bmod p^c$，p 是素數，$c \ge 1$。
我們考慮計算 $n!$，把中間的 p 都除開算出一個值，同時算出除開的 p 的個數。
例如 $n = 19, p = 3, c = 2$，考慮 $19!$：

$$19! = (1 \times 2 \times 4 \times 5 \times 7 \times \cdots \times 16 \times 17 \times 19) \times 3^6 \times (1 \times 2 \times 3 \times \cdots \times 6)$$

令 $f(n)$ 表示 $n!$ 中除去 p 因子後模 p^c 的值。若要求 $f(19)$，那麼就是上式的前半部分，然後 3^6 提出來，最後一部分對答案的貢獻是 $f(6)$，即 $f(\lfloor \frac{n}{p} \rfloor)$。對於前面，又有：

$$1 \times 2 \times 4 \times 5 \times 7 \times 8 \equiv 10 \times 11 \times 13 \times 14 \times 16 \times 17 \pmod 9$$

組合數求模

Solution

最後考慮這麼一種數據範圍，$n, m \le 10^9$，$k \le 10^5$。

首先，我們可以利用中國剩餘定理，可以發現問題等價於求 $C_m^n \bmod p^c$，p 是素數，$c \ge 1$。

我們考慮計算 $n!$，把中間的 p 都除開算出一個值，同時算出除開的 p 的個數。

例如 $n = 19, p = 3, c = 2$，考慮 $19!$：

$$19! = (1 \times 2 \times 4 \times 5 \times 7 \times \cdots \times 16 \times 17 \times 19) \times 3^6 \times (1 \times 2 \times 3 \times \cdots \times 6)$$

令 $f(n)$ 表示 $n!$ 中除去 p 因子後模 p^c 的值。若要求 $f(19)$，那麼就是上式的前半部分，然後 3^6 提出來，最後一部分對答案的貢獻是 $f(6)$，即 $f(\lfloor \frac{n}{p} \rfloor)$。對於前面，又有：

$$1 \times 2 \times 4 \times 5 \times 7 \times 8 \equiv 10 \times 11 \times 13 \times 14 \times 16 \times 17 \pmod 9$$

這是有週期的，而且乘積的項數也不會超過 p^c，所以可以進行預處理。然後從 $f(n)$ 遞歸到 $f(\lfloor \frac{n}{p} \rfloor)$，層數 $O(\log_p n)$。

總結

OI 數論題用到的知識點就那麼幾個，大致的思路可以這個歸納：

OI 數論題用到的知識點就那麼幾個,大致的思路可以這個歸納:

1. 若題目中有模運算,先考慮模素數的情況,再考慮模素數的冪的情況。

總結

OI 數論題用到的知識點就那麼幾個,大致的思路可以這個歸納:

1. 若題目中有模運算,先考慮模素數的情況,再考慮模素數的冪的情況。
2. 預處理素數表和積性函數,求出所有約數,還有各種小定理小算法的應用。

OI 數論題用到的知識點就那麼幾個,大致的思路可以這個歸納:

1. 若題目中有模運算,先考慮模素數的情況,再考慮模素數的冪的情況。
2. 預處理素數表和積性函數,求出所有約數,還有各種小定理小算法的應用。
3. 需要的話,用中國剩餘定理合併答案。

Example (SPOJ_PRIME1)

給出兩個正整數 m 和 n,滿足 $1 \leq m \leq n \leq 10^9$ 且 $n - m \leq 10^5$,輸出所有滿足 $m \leq p \leq n$ 的素數 p。

例子

Example (SPOJ_PRIME1)

給出兩個正整數 m 和 n,滿足 $1 \leq m \leq n \leq 10^9$ 且 $n - m \leq 10^5$,輸出所有滿足 $m \leq p \leq n$ 的素數 p。

Solution

枚舉 $[m, n]$ 上的每個數,用 *Miller-Rabin* 算法判定,時間複雜度 $O((n-m)\log n)$。

Example (SPOJ_PRIME1)

給出兩個正整數 m 和 n,滿足 $1 \leq m \leq n \leq 10^9$ 且 $n - m \leq 10^5$,輸出所有滿足 $m \leq p \leq n$ 的素數 p。

Solution

枚舉 $[m, n]$ 上的每個數,用 *Miller-Rabin* 算法判定,時間複雜度 $O((n - m) \log n)$。

性質利用不充分!

Example (SPOJ_PRIME1)

給出兩個正整數 m 和 n,滿足 $1 \leq m \leq n \leq 10^9$ 且 $n - m \leq 10^5$,輸出所有滿足 $m \leq p \leq n$ 的素數 p。

Solution

枚舉 $[m, n]$ 上的每個數,用 *Miller-Rabin* 算法判定,時間複雜度 $O((n - m) \log n)$。

性質利用不充分!

Solution

由於一個合數必定有一個不超過 $\sqrt{10^9}$ 的約數,所以可以處理出 $\sqrt{10^9}$ 內的素數,然後用這些素數去篩除 $[m, n]$ 上的合數,那麼剩下的就是素數了。時間複雜度略好。

Example (HDU_4059)

給出正整數 n,滿足 $1 \le n \le 10^8$,求 $\sum_{1\le i\le n,(n,i)=1} i^4 \bmod 10^9+7$。

Example (HDU_4059)

給出正整數 n,滿足 $1 \leq n \leq 10^8$,求 $\sum_{1\leq i\leq n,(n,i)=1} i^4 \bmod 10^9+7$。

提示:容斥原理。

Example (HDU_4059)

給出正整數 n,滿足 $1 \le n \le 10^8$,求 $\sum_{1\le i\le n,(n,i)=1} i^4 \bmod 10^9+7$。

提示:容斥原理。

Solution

記 $f(n)=\sum_{1\le i\le n} i^4$,那麼答案就是:

$$\sum_S (-1)^{|S|}(\prod_{p\in S} p)^4 f(\frac{n}{\prod_{p\in S} p})$$

其中,S 是集合 T 的子集,素數 p 屬於集合 T 當且僅當 $p|n$。

例子

Example (Tsinsen_A1369)

求 $ax \equiv 1 \pmod{b}$ 的最小正整數解。

Example (Tsinsen_A1369)

求 $ax \equiv 1 \pmod{b}$ 的最小正整數解。

NOIP2012。

Example (Tsinsen_A1369)

求 $ax \equiv 1 \pmod{b}$ 的最小正整數解。

NOIP2012。

Solution

把方程變形爲 $ax - by = 1$,用擴展歐幾里得算法解決。

例子

Example (Tsinsen_A1369)

求 $ax \equiv 1 \pmod{b}$ 的最小正整數解。

NOIP2012。

Solution

把方程變形爲 $ax - by = 1$,用擴展歐幾里得算法解決。

Solution

在 $(a,b)=1$ 時纔有解,所以由 $a^{\varphi(b)} \equiv 1 \pmod{b}$ 得 $x \equiv a^{\varphi(b)-1} \pmod{b}$。

例子

Example (HYSBZ_2154)

給出正整數 N 和 M,求 $\sum_{i=1}^{N}\sum_{j=1}^{M} lcm(i,j) \bmod 20101009$。$1 \leq N, M \leq 10^7$。

例子

Example (HYSBZ_2154)

給出正整數 N 和 M,求 $\sum_{i=1}^{N}\sum_{j=1}^{M} lcm(i,j) \bmod 20101009$。$1 \leq N, M \leq 10^7$。

難點在於推導。

Example (HYSBZ_2154)

給出正整數 N 和 M,求 $\sum_{i=1}^{N}\sum_{j=1}^{M} lcm(i,j) \bmod 20101009$。$1 \le N, M \le 10^7$。

難點在於推導。

Solution

這裏直接給出推導結果,設 $g(n) = n\sum_{d|n}\mu(d)d$,則答案就是

$$\sum_{t=1}^{N}\frac{1}{4}\lfloor\frac{N}{t}\rfloor\lfloor\frac{M}{t}\rfloor(\lfloor\frac{N}{t}\rfloor+1)(\lfloor\frac{M}{t}\rfloor+1)g(t)$$

易知 $g(n)$ 是積性函數,所以線性篩預處理 g 函數即可。

Example (HDU_2815)

給出方程 $A^x \equiv B \pmod{C}$,求 x 的最小非負整數解。$1 \leq A, B, C \leq 10^9$。

例子

Example (HDU_2815)

給出方程 $A^x \equiv B \pmod{C}$,求 x 的最小非負整數解。$1 \le A, B, C \le 10^9$。

離散對數的經典做法並不適用。

Example (HDU_2815)

給出方程 $A^x \equiv B \pmod{C}$,求 x 的最小非負整數解。$1 \leq A, B, C \leq 10^9$。

離散對數的經典做法並不適用。

Solution

算法失效的原因是 A 和 C 可能不互素。從這個方向切入。

Example (HDU_2815)

給出方程 $A^x \equiv B \pmod{C}$,求 x 的最小非負整數解。$1 \leq A, B, C \leq 10^9$。

離散對數的經典做法並不適用。

Solution

算法失效的原因是 A 和 C 可能不互素。從這個方向切入。

考慮 $A^x = Ct + B$,設 $g = (A, C)$,若 $B \bmod g \neq 0$ 則無解。

所以式子可以化爲 $\frac{A}{g} \cdot A^{x-1} = \frac{C}{g}t + \frac{B}{g}$。相當於是 $\frac{A}{g} \cdot A^{x-1} \equiv \frac{B}{g} \pmod{\frac{C}{g}}$。

例子

Example (HDU_2815)

給出方程 $A^x \equiv B \pmod{C}$,求 x 的最小非負整數解。$1 \le A, B, C \le 10^9$。

離散對數的經典做法並不適用。

Solution

算法失效的原因是 A 和 C 可能不互素。從這個方向切入。

考慮 $A^x = Ct + B$,設 $g = (A, C)$,若 $B \bmod g \ne 0$ 則無解。

所以式子可以化爲 $\frac{A}{g} \cdot A^{x-1} = \frac{C}{g}t + \frac{B}{g}$。相當於是 $\frac{A}{g} \cdot A^{x-1} \equiv \frac{B}{g} \pmod{\frac{C}{g}}$。

反覆進行這個操作 d 次後可以得到 $D \cdot A^y \equiv B' \pmod{C'}, (A, C') = 1$。

那麼可以用經典算法計算出 y,此時 $d + y$ 就是答案。

例子

Example (HDU_2815)

給出方程 $A^x \equiv B \pmod{C}$,求 x 的最小非負整數解。$1 \le A, B, C \le 10^9$。

離散對數的經典做法並不適用。

Solution

算法失效的原因是 A 和 C 可能不互素。從這個方向切入。

考慮 $A^x = Ct + B$,設 $g = (A, C)$,若 $B \bmod g \neq 0$ 則無解。

所以式子可以化爲 $\frac{A}{g} \cdot A^{x-1} = \frac{C}{g}t + \frac{B}{g}$。相當於是 $\frac{A}{g} \cdot A^{x-1} \equiv \frac{B}{g} \pmod{\frac{C}{g}}$。

反覆進行這個操作 d 次後可以得到 $D \cdot A^y \equiv B' \pmod{C'}, (A, C') = 1$。

那麼可以用經典算法計算出 y,此時 $d + y$ 就是答案。

有沒有什麼問題?

Example (HDU_2815)

給出方程 $A^x \equiv B \pmod{C}$,求 x 的最小非負整數解。$1 \le A, B, C \le 10^9$。

離散對數的經典做法並不適用。

Solution

算法失效的原因是 A 和 C 可能不互素。從這個方向切入。

考慮 $A^x = Ct + B$,設 $g = (A, C)$,若 $B \bmod g \ne 0$ 則無解。

所以式子可以化爲 $\frac{A}{g} \cdot A^{x-1} = \frac{C}{g}t + \frac{B}{g}$。相當於是 $\frac{A}{g} \cdot A^{x-1} \equiv \frac{B}{g} \pmod{\frac{C}{g}}$。

反覆進行這個操作 d 次後可以得到 $D \cdot A^y \equiv B' \pmod{C'}, (A, C') = 1$。

那麼可以用經典算法計算出 y,此時 $d + y$ 就是答案。

有沒有什麼問題?

Solution

考慮可能有小於 d 的解,所以需要枚舉小於 d 的非負整數 x 去判斷。因爲易知 d 是 $O(\log N)$ 級別的,所以算法可行。

Example (HYSBZ_2219)

給出方程 $x^A \equiv B \pmod{C}$,求 x 在 $[0, C)$ 上的整數解的個數。
$1 \leq A, B, C \leq 10^9$,且 C 是奇數。

例子

Example (HYSBZ_2219)

給出方程 $x^A \equiv B \pmod{C}$,求 x 在 $[0, C)$ 上的整數解的個數。
$1 \le A, B, C \le 10^9$,且 C 是奇數。

中國剩餘定理的一個推論:方程組 $f_i(x) \equiv 0 \pmod{m_i}$, m_i 兩兩 ˙ 互素,若第 i 個方程在 $[0, m_i)$ 上的解數是 t_i,則方程組在 $[0, \prod m_i)$ 上的解數是 $\prod t_i$。

Example (HYSBZ_2219)

給出方程 $x^A \equiv B \pmod{C}$,求 x 在 $[0, C)$ 上的整數解的個數。
$1 \le A, B, C \le 10^9$,且 C 是奇數。

中國剩餘定理的一個推論:方程組 $f_i(x) \equiv 0 \pmod{m_i}$,$m_i$ 兩兩˙互素,若第 i 個方程在 $[0, m_i)$ 上的解數是 t_i,則方程組在 $[0, \prod m_i)$ 上的解數是 $\prod t_i$。

Solution

問題轉化爲 $x^A \ equivB \pmod{p^k}$,p 是一個奇素數。
分三種情況討論:

- $B \equiv 0 \pmod{p^k}$
- $(B, p^k) > 1$
- $(B, p^k) = 1$

Solution

先看 $B \equiv 0 \pmod{p^k}$。

Solution

先看 $B \equiv 0 \pmod{p^k}$。

即 $x^A \equiv 0 \pmod{p^k}$,所以 x 中 p 因子的次數至少是 $\lceil \frac{k}{A} \rceil$。於是解數是 $\frac{p^k}{p^{\lceil \frac{k}{A} \rceil}} = p^{k-\lceil \frac{k}{A} \rceil}$。

例子

Solution

先看 $B \equiv 0 \pmod{p^k}$。

即 $x^A \equiv 0 \pmod{p^k}$,所以 x 中 p 因子的次數至少是 $\lceil \frac{k}{A} \rceil$。於是解數是 $\frac{p^k}{p^{\lceil \frac{k}{A} \rceil}} = p^{k-\lceil \frac{k}{A} \rceil}$。

Solution

再来看 $(B, p^k) > 1$ 的情況。

例子

Solution

先看 $B \equiv 0 \pmod{p^k}$。
即 $x^A \equiv 0 \pmod{p^k}$,所以 x 中 p 因子的次數至少是 $\lceil \frac{k}{A} \rceil$。於是解數是 $\frac{p^k}{p^{\lceil \frac{k}{A} \rceil}} = p^{k-\lceil \frac{k}{A} \rceil}$。

Solution

再来看 $(B, p^k) > 1$ 的情況。
則可以設 $B = p^r \cdot b$,其中 b 不含因子 p,則有 $x^A \equiv p^r \cdot b \pmod{p^k}$。有解的條件是 $A | r$,於是 $(p^{\frac{r}{A}} \cdot y)^A \equiv p^r \cdot b \pmod{p^k}$。

Solution

先看 $B \equiv 0 \pmod{p^k}$。
即 $x^A \equiv 0 \pmod{p^k}$,所以 x 中 p 因子的次數至少是 $\lceil \frac{k}{A} \rceil$。於是解數是 $\frac{p^k}{p^{\lceil \frac{k}{A} \rceil}} = p^{k-\lceil \frac{k}{A} \rceil}$。

Solution

再来看 $(B, p^k) > 1$ 的情況。
則可以設 $B = p^r \cdot b$,其中 b 不含因子 p,則有 $x^A \equiv p^r \cdot b \pmod{p^k}$。有解的條件是 $A|r$,於是 $(p^{\frac{r}{A}} \cdot y)^A \equiv p^r \cdot b \pmod{p^k}$。
兩邊消去 p^r 得到 $y^A \equiv b \pmod{p^{k-r}}$,此時 $(b, p^{k-r}) = 1$,轉化爲第三種情況。

Solution

最後第三種情況,$(B, p^k) = 1$。

Solution

最後第三種情況,$(B, p^k) = 1$。
由於 p 是奇素數,所以模 p^k 具有原根,設原根爲 g。對方程兩邊取離散對數,有
$A \cdot ind_g x \equiv ind_g b \pmod{\varphi(p^k)}$。

Solution

最後第三種情況,$(B, p^k) = 1$。

由於 p 是奇素數,所以模 p^k 具有原根,設原根爲 g。對方程兩邊取離散對數,有

$A \cdot ind_g x \equiv ind_g b \pmod{\varphi(p^k)}$。

如果 $ind_g b$ 存在的話,解數就是 $gcd(A, \varphi(p^k))$。

例子

Example (POJ_3146)

給出非負整數 N 和素數 P,統計 C_x^N 中有多少個不是 P 的倍數。
$N \leq 10^9, P < 1000$。

Example (POJ_3146)

給出非負整數 N 和素數 P,統計 C_x^N 中有多少個不是 P 的倍數。
$N \leq 10^9, P < 1000$。

Solution

根據 *Lucas* 定理,若 $C_x^N \bmod P$ 爲 0,那麼 N 在 P 進制下某一位一定有 $x_i > N_i$,反之,若不爲 0,則每一位都不超過 N_i,所以答案就是 $\prod_i N_i + 1$。

Example (HYSBZ_1951)

這道題目描述太醜了，這裏直接給出要求的式子：

$$G^{\sum_{i|N} C_i^N} \bmod 999911659$$

其中 $1 \leq G, N \leq 10^9$。

Example (HYSBZ_1951)

這道題目描述太醜了,這裏直接給出要求的式子:

$$G^{\sum_{i|N} C_i^N} \bmod 999911659$$

其中 $1 \leq G, N \leq 10^9$。

提示:999911659 是素數,且 $999911658 = 2 \times 3 \times 4679 \times 35617$。

Example (HYSBZ_1951)

這道題目描述太醜了,這裏直接給出要求的式子:

$$G^{\sum_{i|N} C_i^N} \bmod 999911659$$

其中 $1 \leq G, N \leq 10^9$。

提示:999911659 是素數,且 $999911658 = 2 \times 3 \times 4679 \times 35617$。

Solution

令 $P = 999911659$,則由 P 是素數知 $G^x \equiv G^{x \bmod (P-1)} \pmod P$。

令 $Q = P - 1$,則問題轉化成,求 $\sum_{i|N} C_i^N \bmod Q$。

例子

Example (HYSBZ_1951)

這道題目描述太醜了,這裏直接給出要求的式子:

$$G^{\sum_{i|N} C_i^N} \bmod 999911659$$

其中 $1 \leq G, N \leq 10^9$。

提示:999911659 是素數,且 $999911658 = 2 \times 3 \times 4679 \times 35617$。

Solution

令 $P = 999911659$,則由 P 是素數知 $G^x \equiv G^{x \bmod (P-1)} \pmod P$。

令 $Q = P - 1$,則問題轉化成,求 $\sum_{i|N} C_i^N \bmod Q$。

枚舉 N 的約數的複雜度是可以接受的,問題就變成求 $C_x^N \bmod Q$,在這個問題中 N, x, Q 都比較大,但 Q 的每個因子並不大。於是對每個因子用 *Lucas* 定理求答案,最後用中國剩餘定理合併。