数论

Number Theory

何中天

2018 年 6 月 8 日

自我介绍

NOIP2013-2017提高一等，4次入选北京省队。

NOI2016金牌，APIO2016金牌第6名，国际银牌，CCO2016金牌第3名（加拿大国赛）。

WC15、16金牌，CTSC16金牌。

NOI2017金牌第3名。

2018年中国国家队15人候选队。

初等数论简介

数论是纯粹数学的分支之一，主要研究整数的性质。

初等数论简介

数论是纯粹数学的分支之一，主要研究整数的性质。

初等数论主要就是研究整数环的整除理论及同余理论。此外它也包括了连分数理论和少许不定方程的问题。本质上说，初等数论的研究手段局限在整除性质上。

初等数论简介

数论是纯粹数学的分支之一，主要研究整数的性质。

初等数论主要就是研究整数环的整除理论及同余理论。此外它也包括了连分数理论和少许不定方程的问题。本质上说，初等数论的研究手段局限在整除性质上。

初等数论中经典的结论包括算术基本定理、欧几里得的质数无限证明、中国剩余定理、欧拉定理（其特例是费马小定理）、高斯的二次互反律、商高定理、佩尔方程的连分数求解法等等。

初等数论简介

数论是纯粹数学的分支之一，主要研究整数的性质。

初等数论主要就是研究整数环的整除理论及同余理论。此外它也包括了连分数理论和少许不定方程的问题。本质上说，初等数论的研究手段局限在整除性质上。

初等数论中经典的结论包括算术基本定理、欧几里得的质数无限证明、中国剩余定理、欧拉定理（其特例是费马小定理）、高斯的二次互反律、商高定理、佩尔方程的连分数求解法等等。

应用：密码学，hash算法等。

数论的一些著名猜想

- 哥德巴赫猜想：是否每个大于2的偶数都可写成两个质数之和？
- 孪生素数猜想：孪生素数就是差为2的素数对，例如11和13。是否存在无穷多的孪生素数
- 斐波那契数列内是否存在无穷多的素数？
- 是否存在无穷多的梅森素数？
- 费马猜想（费马大定理），1995年怀尔斯和理查・泰勒证明了历时350年的费马猜想。
- 黎曼猜想

整除

Definition

对于整数n, m，如果$m \neq 0$且存在整数k，使得$km = n$，我们就称m整除n（或者n被m整除），m是n的约数，n是m的倍数。

整除

Definition

对于整数n, m，如果$m \neq 0$且存在整数k，使得$km = n$，我们就称m整除n（或者n被m整除），m是n的约数，n是m的倍数。

这个性质奠定了整个数论的基础，所以赋予它一个特殊记号会更方便，记为$m \mid n$。

整除

Definition

对于整数n, m，如果$m \neq 0$且存在整数k，使得$km = n$，我们就称m整除n（或者n被m整除），m是n的约数，n是m的倍数。

这个性质奠定了整个数论的基础，所以赋予它一个特殊记号会更方便，记为$m \mid n$。

整除有很多性质，比如

- 自反性：$a \mid a \ (a \neq 0)$
- 对称性：若$a \mid b, b \mid a$，则$a = \pm b$
- 传递性：如果$a \mid b$，$b \mid c$，那么$a \mid c$。
- 设$b \neq 0$，如果$a|b$，则$|a| \leq |b|$
- $b \mid a \iff bm \mid am$（m是非零整数）。
- $a \mid b$且$a \mid c \iff$ 对任意两个整数x, y都有$a \mid bx + cy$。

整除

我们举例证明其中两条：

- 如果$a \mid b$，$b \mid c$，那么$a \mid c$。

整除

我们举例证明其中两条：

- 如果$a \mid b$，$b \mid c$，那么$a \mid c$。
  因为$b = ka, c = mb(k, m \in \mathbb{Z})$，所以$c = mka$。

整除

我们举例证明其中两条：

- 如果$a \mid b$，$b \mid c$，那么$a \mid c$。
  因为$b = ka, c = mb(k, m \in \mathbb{Z})$，所以$c = mka$。
- $a \mid b$且$a \mid c \iff$ 对任意两个整数x, y都有$a \mid bx + cy$。

整除

我们举例证明其中两条：

- 如果$a \mid b$，$b \mid c$，那么$a \mid c$。
  因为$b = ka, c = mb(k, m \in \mathbb{Z})$，所以$c = mka$。
- $a \mid b$且$a \mid c \iff$ 对任意两个整数x, y都有$a \mid bx + cy$。
  左边推出右边：
  设$b = ka, c = la$，对于任意两个整数x, y都有$bx = kxa, cy = lya$，
  相加得：$bx + cy = (kx + ly)a$，故$a \mid bx + cy$。

整除

我们举例证明其中两条：

- 如果$a \mid b$，$b \mid c$，那么$a \mid c$。
  因为$b = ka, c = mb(k, m \in \mathbb{Z})$，所以$c = mka$。
- $a \mid b$且$a \mid c \iff$ 对任意两个整数x, y都有$a \mid bx + cy$。
  左边推出右边：
  设$b = ka, c = la$，对于任意两个整数x, y都有$bx = kxa, cy = lya$，
  相加得：$bx + cy = (kx + ly)a$，故$a \mid bx + cy$。
  右边推出左边：
  因为对任意两个整数x, y都有$bx + cy = ka$，

整除

我们举例证明其中两条：

- 如果$a \mid b$，$b \mid c$，那么$a \mid c$。
  因为$b = ka, c = mb (k, m \in \mathbb{Z})$，所以$c = mka$。
- $a \mid b$且$a \mid c \iff$ 对任意两个整数x, y都有$a \mid bx + cy$。
  左边推出右边：
  设$b = ka, c = la$，对于任意两个整数x, y都有$bx = kxa, cy = lya$，
  相加得：$bx + cy = (kx + ly)a$，故$a \mid bx + cy$。
  右边推出左边：
  因为对任意两个整数x, y都有$bx + cy = ka$，
  当$x = 1, y = 0$时，$b = ka$，故$a \mid b$。
  当$x = 0, y = 1$时，$c = ka$，故$a \mid c$。

素数

Definition

一个大于1的正整数，除了1和它自身外，不能被其他正整数整除的数叫做素数；否则称为合数。

素数

Definition

一个大于1的正整数，除了1和它自身外，不能被其他正整数整除的数叫做素数；否则称为合数。

素数有无限多个。

欧几里得的《几何原本》中有一个经典的证明。它使用了证明常用的方法：反证法。

素数

Definition

一个大于1的正整数，除了1和它自身外，不能被其他正整数整除的数叫做素数；否则称为合数。

素数有无限多个。

欧几里得的《几何原本》中有一个经典的证明。它使用了证明常用的方法：反证法。

Theorem (素数定理)

当x很大时，小于x的素数的个数近似等于$x/ln(x)$。

Theorem (算术基本定理)

任何一个大于1的正整数n，都可以唯一分解成有限个素数的乘积。

$$n = p_1 p_2 \cdots p_m = \prod_{k=1}^{m} p_k, \ p_1 \leq \cdots \leq p_m.$$

算术基本定理也可以写成 $n = p_1^{r_1} \cdot p_2^{r_2} \cdots p_k^{r_k}$

素数判定

给一个正整数 n，如何判定它是否为素数？

素数判定

给一个正整数 n，如何判定它是否为素数？ 试除法!

解法0：枚举从 2 到 $n-1$ 的所有正整数，检查整除性，时间复杂度 $O(n)$。

素数判定

给一个正整数 n，如何判定它是否为素数？ 试除法!

解法0：枚举从 2 到 $n-1$ 的所有正整数，检查整除性，时间复杂度 $O(n)$。

解法1：枚举从 2 到 $\sqrt{n}$ 的所有正整数，检查整除性，时间复杂度 $O(\sqrt{n})$。

假设一个数能整除n，即$a \mid n$，那么n/a也必定能整除n，不妨设$a \leq n/a$（否则可令$a = n/a$），则有$a^2 \leq n$，即$a \leq \sqrt{n}$。

给一个正整数 n，如何判定它是否为素数？ 试除法!

解法0：枚举从 2 到 $n-1$ 的所有正整数，检查整除性，时间复杂度 $O(n)$。

解法1：枚举从 2 到 $\sqrt{n}$ 的所有正整数，检查整除性，时间复杂度 $O(\sqrt{n})$。

假设一个数能整除n，即$a \mid n$，那么n/a也必定能整除n，不妨设$a \leq n/a$（否则可令$a = n/a$），则有$a^2 \leq n$，即$a \leq \sqrt{n}$。

如果 n 是合数，那么它必然有一个小于等于$\sqrt{n}$的素因子。

解法2：枚举从 2 到 $\sqrt{n}$ 的所有素因子，检查整除性，单次时间复杂度 $O(\sqrt{n}/ln(n))$。

素数判定

给一个正整数 n，如何判定它是否为素数？ 试除法!

解法0：枚举从 2 到 $n-1$ 的所有正整数，检查整除性，时间复杂度 $O(n)$。

解法1：枚举从 2 到 $\sqrt{n}$ 的所有正整数，检查整除性，时间复杂度 $O(\sqrt{n})$。

假设一个数能整除n，即$a \mid n$，那么n/a也必定能整除n，不妨设$a \leq n/a$（否则可令$a = n/a$），则有$a^2 \leq n$，即$a \leq \sqrt{n}$。

如果 n 是合数，那么它必然有一个小于等于$\sqrt{n}$的素因子。

解法2：枚举从 2 到 $\sqrt{n}$ 的所有素因子，检查整除性，单次时间复杂度 $O(\sqrt{n}/ln(n))$。

解法3：Miller-Rabin素性测试。

质因数分解

还是利用性质：如果 n 是合数，那么它必然有一个小于等于$\sqrt{n}$的素因子。

从 2 到 $\sqrt{n}$ 枚举试除，对于一个因子不断除直到除净。

最后可能会留有一个大的素因子。

因子

朴素的求因子的方法为枚举$[1,n]$的数进行整除判定，复杂度为$O(n)$。加入一个优化，如果m为n的因子，那么必然n/m也为n的因子，不妨设$m \leq n/m$，则有$m \leq \sqrt{n}$，所以只要从$[1,\sqrt{n}]$枚举即可，注意特判$x^2 = n$（不要重复计算），复杂度$O(\sqrt{n})$。

$n = p_1^{r_1} \cdot p_2^{r_2} \cdots p_k^{r_k}$ 由乘法计数原理得，约数个数为$(r_1+1)\cdot(r_2+1)\cdots(r_k+1)$

筛法

Example

给一个正整数 n，求出不超过 n 的所有素数。

埃拉托斯特尼筛法：逐次枚举 2 到 n，设当前枚举到 x，如果x没有被标记过，那么x是素数，并将x的倍数标记为“非素数”。

筛法

Example

给一个正整数 n，求出不超过 n 的所有素数。

埃拉托斯特尼筛法：逐次枚举 2 到 n，设当前枚举到 x，如果x没有被标记过，那么x是素数，并将x的倍数标记为“非素数”。

线性筛法：逐次枚举 2 到 n，并且记录下当前找到的所有素数。然后每处理到一个数x，从小到大枚举所有当前找到的素数，将其与x的乘积剔除。直到x被当前枚举的素数整除为止。

给定$n(n < 10000)$个数，范围为$[1, 2^{32})$，判定它们是素数还是合数。

给定$n(n < 10000)$个数，范围为$[1, 2^{32})$，判定它们是素数还是合数。

首先1不是素数，如果$n > 1$，则枚举$[1, \sqrt{x}]$范围内的素数进行试除

$[1, \sqrt{M}]$范围内的素数可以通过筛法预先筛出来。

区间筛

SPOJ PRIME1：

给定$l, r(1 \leq l \leq r \leq 10^9, r - l < 10^5)$，求$[l, r]$范围内的素数。

区间筛

SPOJ PRIME1：

给定$l, r(1 \le l \le r \le 10^9, r - l < 10^5)$，求$[l, r]$范围内的素数。

枚举$[1, \sqrt{r}]$范围内的素数来筛。

$[1, \sqrt{r}]$范围内的素数可以通过筛法预先筛出来。

区间筛

SPOJ PRIME1：

给定$l, r(1 \le l \le r \le 10^9, r - l < 10^5)$，求$[l, r]$范围内的素数。

枚举$[1, \sqrt{r}]$范围内的素数来筛。

$[1, \sqrt{r}]$范围内的素数可以通过筛法预先筛出来。

也可以枚举 $[m, n]$ 上的每个数，用 Miller-Rabin 算法判定，没有充分利用题目性质。

mod运算

mod的定义来自带余除法。

Theorem (除法定理)

如果n, m是两个整数，$m \neq 0$，存在唯一一对整数q和r，满足$n = qm + r$且$0 \leq r < |m|$

mod运算

mod的定义来自带余除法。

Theorem (除法定理)

如果n, m是两个整数，$m \neq 0$，存在唯一一对整数q和r，满足$n = qm + r$且$0 \leq r < |m|$

称$q = \lfloor n/m \rfloor$为除法的**商**，值$r = n \bmod m$为除法的**余数**。

也就是$n = m\lfloor n/m \rfloor + n \bmod m, m \neq 0$

mod运算

mod的定义来自带余除法。

Theorem (除法定理)

如果n, m是两个整数，$m \neq 0$，存在唯一一对整数q和r，满足$n = qm + r$且$0 \leq r < |m|$

称$q = \lfloor n/m \rfloor$为除法的**商**，值$r = n \bmod m$为除法的**余数**。

也就是$n = m\lfloor n/m \rfloor + n \bmod m, m \neq 0$

可得$n \bmod m = n - m\lfloor n/m \rfloor, m \neq 0$

mod运算

mod的定义来自带余除法。

Theorem (除法定理)

如果n, m是两个整数，$m \neq 0$，存在唯一一对整数q和r，满足$n = qm + r$且$0 \leq r < |m|$

称$q = \lfloor n/m \rfloor$为除法的**商**，值$r = n \bmod m$为除法的**余数**。

也就是$n = m\lfloor n/m \rfloor + n \bmod m, m \neq 0$

可得$n \bmod m = n - m\lfloor n/m \rfloor, m \neq 0$

这就将mod定义成为一个二元运算，该定义当n, m是实数时也有意义，不过在数论中我们通常只对整数用此定义。

最大公约数

Definition

两个整数m和n的最大公约数是能整除它们两者的最大整数。记为$\gcd(m, n)$或(m, n)。

gcd最好的性质之一是它容易计算，可以用有2300年之久的欧几里得算法来计算它。

最大公约数

Definition

两个整数m和n的最大公约数是能整除它们两者的最大整数。记为$\gcd(m,n)$或(m,n)。

gcd最好的性质之一是它容易计算，可以用有2300年之久的欧几里得算法来计算它。

对于$0 \leq m < n$计算$\gcd(n,m)$，欧几里得算法用到递归式

$$\gcd(0,n) = n;$$
$$\gcd(m,n) = \gcd(n \bmod m, m), m > 0.$$

Theorem (GCD递归定理)

对任意非负整数a和正整数b，$\gcd(a, b) = \gcd(b, a \bmod b)$。

Theorem (GCD递归定理)

对任意非负整数a和正整数b，$\gcd(a, b) = \gcd(b, a \bmod b)$。

只需要证明上面两者能相互整除。

Theorem (GCD递归定理)

对任意非负整数a和正整数b，$\gcd(a,b)=\gcd(b, a \bmod b)$。

只需要证明上面两者能相互整除。

设$\gcd(a,b)=d$所以$d \mid a$且$d \mid b$。由带余除法可以得出：$a \bmod b = a - qb$，其中$q=\lfloor a/b \rfloor$。所以$a \bmod b$是a和b的一个线性组合，所以$d \mid a \bmod b$。又因为$d \mid b$，所以$d \mid \gcd(b, a \bmod b)$，即$\gcd(a,b) \mid \gcd(b, a \bmod b)$。

Theorem (GCD递归定理)

对任意非负整数a和正整数b，$\gcd(a,b)=\gcd(b, a \bmod b)$。

只需要证明上面两者能相互整除。

设$\gcd(a,b)=d$所以$d \mid a$且$d \mid b$。由带余除法可以得出：$a \bmod b = a - qb$，其中$q=\lfloor a/b \rfloor$。所以$a \bmod b$是a和b的一个线性组合，所以$d \mid a \bmod b$。又因为$d \mid b$，所以$d \mid \gcd(b, a \bmod b)$，即$\gcd(a,b) \mid \gcd(b, a \bmod b)$。

证明$\gcd(b, a \bmod b) \mid \gcd(a,b)$和上述过程几乎一样。

裴蜀定理

Theorem

对任何$a, b \in Z$和它们的最大公约数d，关于未知数x和y的线性不定方程（称为裴蜀等式）：$ax + by = c$有整数解(x, y)当且仅当$d \mid c$，可知有无穷多解。特别地，一定存在整数x, y，使$ax + by = d$成立。

裴蜀定理

Theorem

对任何$a, b \in Z$和它们的最大公约数d，关于未知数x和y的线性不定方程（称为裴蜀等式）：$ax + by = c$有整数解(x, y)当且仅当$d \mid c$，可知有无穷多解。特别地，一定存在整数x, y，使$ax + by = d$成立。

Lemma

a与b的线性组合集中最小的正元素是$\gcd(a, b)$。

裴蜀定理

Theorem

对任何$a, b \in Z$和它们的最大公约数d，关于未知数x和y的线性不定方程（称为裴蜀等式）：$ax + by = c$有整数解(x, y)当且仅当$d \mid c$，可知有无穷多解。特别地，一定存在整数x, y，使$ax + by = d$成立。

Lemma

a与b的线性组合集中最小的正元素是$\gcd(a, b)$。

设s是a与b的线性组合集中最小的正元素，对于某个$x, y \in Z$，有$s = ax + by$。 设$q = \lfloor a/s \rfloor$，则有

$r = a \ mod \ s = a - qs = a - q(ax + by) = a(1 - qx) + b(-qy)$

因此r也是a与b的一个线性组合，由于s是这个线性集合中的最小正整数，又$0 \leq r < s$，可得$r = 0$，因此有$s \mid a$，同理有$s \mid b$，因此s是a 与b的公约数，所以有$d \geq s$。其实用扩欧就能得出存在等于d的线性组合。

裴蜀定理

Theorem

对任何$a, b \in Z$和它们的最大公约数d，关于未知数x和y的线性不定方程（称为裴蜀等式）：$ax + by = c$有整数解(x, y)当且仅当$d \mid c$，可知有无穷多解。特别地，一定存在整数x, y，使$ax + by = d$成立。

Lemma

a与b的线性组合集中最小的正元素是$\gcd(a, b)$。

设s是a与b的线性组合集中最小的正元素，对于某个$x, y \in Z$，有$s = ax + by$。设$q = \lfloor a/s \rfloor$，则有

$r = a \bmod s = a - qs = a - q(ax + by) = a(1 - qx) + b(-qy)$

因此r也是a与b的一个线性组合，由于s是这个线性集合中的最小正整数，又$0 \le r < s$，可得$r = 0$，因此有$s \mid a$，同理有$s \mid b$，因此s是a 与b的公约数，所以有$d \ge s$。其实用扩欧就能得出存在等于d的线性组合。

因为对于任意$x, y \in Z$，有$d \mid (ax + by)$，所以有$d \mid s$。由于$d \mid s$且$s > 0$，可得$d \le s$。综合$d \le s$和$d \ge s$，得$d = s$，故$s = \gcd(a, b)$。

裴蜀定理

Theorem

对任何$a, b \in Z$和它们的最大公约数d，关于未知数x和y的线性不定方程（称为裴蜀等式）：$ax + by = c$有整数解(x, y)当且仅当$d \mid c$，可知有无穷多解。特别地，一定存在整数x, y，使$ax + by = d$成立。

我们已经证明了a与b的线性组合集中最小的正元素是$\gcd(a, b)$。

裴蜀定理

Theorem

对任何$a, b \in Z$和它们的最大公约数d，关于未知数x和y的线性不定方程（称为裴蜀等式）：$ax + by = c$有整数解(x, y)当且仅当$d \mid c$，可知有无穷多解。特别地，一定存在整数x, y，使$ax + by = d$成立。

我们已经证明了a与b的线性组合集中最小的正元素是$\gcd(a, b)$。

充分性：已知$ax + by = d$一定有整数解，设其解为(x_0, y_0)。$d \mid c$，则存在$k \in Z$，使得$c = kd = k(ax + by) = a(kx) + b(ky)$，即解为$(kx_0, ky_0)$。

裴蜀定理

Theorem

对任何$a, b \in Z$和它们的最大公约数d，关于未知数x和y的线性不定方程（称为裴蜀等式）：$ax + by = c$有整数解(x, y)当且仅当$d \mid c$，可知有无穷多解。特别地，一定存在整数x, y，使$ax + by = d$成立。

我们已经证明了a与b的线性组合集中最小的正元素是$\gcd(a, b)$。

充分性：已知$ax + by = d$一定有整数解，设其解为(x_0, y_0)。$d \mid c$，则存在$k \in Z$，使得$c = kd = k(ax + by) = a(kx) + b(ky)$，即解为$(kx_0, ky_0)$。

必要性：$d \mid a$，$d \mid b$，$d \mid ax + by$，所以$d \mid c$。

裴蜀定理可以从二元拓展到多元。

裴蜀定理

Theorem

对任何$a, b \in Z$和它们的最大公约数d，关于未知数x和y的线性不定方程（称为裴蜀等式）：$ax + by = c$有整数解(x, y)当且仅当$d \mid c$，可知有无穷多解。特别地，一定存在整数x, y，使$ax + by = d$成立。

我们已经证明了a与b的线性组合集中最小的正元素是$\gcd(a, b)$。

充分性：已知$ax + by = d$一定有整数解，设其解为(x_0, y_0)。$d \mid c$，则存在$k \in Z$，使得$c = kd = k(ax + by) = a(kx) + b(ky)$，即解为$(kx_0, ky_0)$。

必要性：$d \mid a$，$d \mid b$，$d \mid ax + by$，所以$d \mid c$。

裴蜀定理可以从二元拓展到多元。

Corollary

对任意整数a与b，如果$d \mid a$且$d \mid b$，则$d \mid \gcd(a, b)$。

裴蜀定理

Theorem

对任何$a, b \in Z$和它们的最大公约数d，关于未知数x和y的线性不定方程（称为裴蜀等式）：$ax + by = c$有整数解(x, y)当且仅当$d \mid c$，可知有无穷多解。特别地，一定存在整数x, y，使$ax + by = d$成立。

我们已经证明了a与b的线性组合集中最小的正元素是$\gcd(a, b)$。

充分性：已知$ax + by = d$一定有整数解，设其解为(x_0, y_0)。$d \mid c$，则存在$k \in Z$，使得$c = kd = k(ax + by) = a(kx) + b(ky)$，即解为$(kx_0, ky_0)$。

必要性：$d \mid a$，$d \mid b$，$d \mid ax + by$，所以$d \mid c$。

裴蜀定理可以从二元拓展到多元。

Corollary

对任意整数a与b，如果$d \mid a$且$d \mid b$，则$d \mid \gcd(a, b)$。

因为$gcd(a, b)$是a与b的一个线性组合，所以$d \mid \gcd(a, b)$。

Corollary

a与b互质的充要条件是，存在整数x, y，使得$ax + by = 1$。

Corollary

a与b互质的充要条件是，存在整数x, y，使得$ax + by = 1$。

Corollary

若$a \mid bc$，且$(a, b) = 1$，则$a \mid c$。

Corollary

a与b互质的充要条件是，存在整数x, y，使得$ax + by = 1$。

Corollary

若$a \mid bc$，且$(a, b) = 1$，则$a \mid c$。

存在整数m, n，使得$am + bn = 1$。于是$acm + bcn = c$。又因为$a \mid ac, a \mid bc$。所以$a \mid acm + bcn$，即$a \mid c$。

Corollary

a与b互质的充要条件是，存在整数x, y，使得$ax + by = 1$。

Corollary

若$a \mid bc$，且$(a, b) = 1$，则$a \mid c$。

存在整数m, n，使得$am + bn = 1$。于是$acm + bcn = c$。又因为$a \mid ac, a \mid bc$。所以$a \mid acm + bcn$，即$a \mid c$。

Corollary

若质数$p \mid ab$，则$p \mid a$或$p \mid b$。

Corollary

a与b互质的充要条件是，存在整数x, y，使得$ax + by = 1$。

Corollary

若$a \mid bc$，且$(a, b) = 1$，则$a \mid c$。

存在整数m, n，使得$am + bn = 1$。于是$acm + bcn = c$。又因为$a \mid ac, a \mid bc$。所以$a \mid acm + bcn$，即$a \mid c$。

Corollary

若质数$p \mid ab$，则$p \mid a$或$p \mid b$。

只有两种情况$(a, p) = p$或$(a, p) = 1$，第一种就是$p \mid a$，第二种由上一个性质得$p \mid b$。

素数的这条性质可以推广到一般情形，若$p \mid a_1 a_2 \cdots a_k$，则存在$a_i$使得$p \mid a_i$。

素数 算术基本定理

Theorem (算术基本定理)

任何一个大于1的正整数数n，都可以唯一分解成有限个素数的乘积。

$$n = p_1 \cdots p_m = \prod_{k=1}^{m} p_k，\ p_1 \leq \cdots \leq p_m.$$

素数 算术基本定理

Theorem (算术基本定理)

任何一个大于1的正整数数n，都可以唯一分解成有限个素数的乘积。

$$n = p_1 \cdots p_m = \prod_{k=1}^{m} p_k, \; p_1 \le \cdots \le p_m.$$

我们分别证明存在性和唯一性。

Theorem (算术基本定理)

任何一个大于1的正整数数n，都可以唯一分解成有限个素数的乘积。

$$n = p_1 \cdots p_m = \prod_{k=1}^{m} p_k,\ p_1 \leq \cdots \leq p_m.$$

我们分别证明存在性和唯一性。

存在性。因为如果$n > 1$不是素数，那么他就有一个因子$n1$，使得$1 < n_1 < n$，这样我们就能写成$n = n_1 n_2$，而（根据归纳法）我们知道n_1和n_2可以写成素数的乘积。

Theorem (算术基本定理)

任何一个大于1的正整数数n，都可以唯一分解成有限个素数的乘积。

$$n = p_1 \cdots p_m = \prod_{k=1}^{m} p_k,\ p_1 \leq \cdots \leq p_m.$$

我们分别证明存在性和唯一性。

存在性。因为如果$n > 1$不是素数，那么他就有一个因子$n1$，使得$1 < n_1 < n$，这样我们就能写成$n = n_1 n_2$，而（根据归纳法）我们知道n_1和n_2可以写成素数的乘积。

唯一性。反证法：假设n有两种方法分解，

$n = p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_s$。用到我们刚得出的引理：

若$p \mid a_1 a_2 \cdots a_k$，则存在$a_i$使得$p \mid a_i$。因为$p_1 \mid q_1 q_2 \cdots q_s$所以存在$q_i$使得$p_1 \mid q_i$，又因为$q_i$也是质数，所以$p_1 = q_i$，同时除掉之后由归纳法即可得证。

算术基本定理

由算术基本定理 $n = p_1^{r_1} \cdot p_2^{r_2} \cdots p_k^{r_k}$

两个数相乘就等价于指数表示相加。

$$k = mn \iff k_p = m_p + n_p\text{，对所有}p$$

算术基本定理

由算术基本定理 $n = p_1^{r_1} \cdot p_2^{r_2} \cdots p_k^{r_k}$
两个数相乘就等价于指数表示相加。

$$k = mn \iff k_p = m_p + n_p\text{，对所有}\, p$$

这就蕴含

$$m \mid n \iff m_p \leq n_p\text{，对所有}\, p$$

算术基本定理

由算术基本定理 $n = p_1^{r_1} \cdot p_2^{r_2} \cdots p_k^{r_k}$
两个数相乘就等价于指数表示相加。

$$k = mn \iff k_p = m_p + n_p，\text{对所有} p$$

这就蕴含

$$m \mid n \iff m_p \leq n_p，\text{对所有} p$$

由此可以立即推出

$$k = \gcd(m, n) \iff k_p = \min(m_p, n_p)，\text{对所有} p$$

$$k = \operatorname{lcm}(m, n) \iff k_p = \max(m_p, n_p)，\text{对所有} p$$

算术基本定理

由算术基本定理 $n = p_1^{r_1} \cdot p_2^{r_2} \cdots p_k^{r_k}$
两个数相乘就等价于指数表示相加。

$$k = mn \iff k_p = m_p + n_p\text{，对所有}p$$

这就蕴含

$$m \mid n \iff m_p \le n_p\text{，对所有}p$$

由此可以立即推出

$$k = \gcd(m, n) \iff k_p = \min(m_p, n_p)\text{，对所有}p$$

$$k = \operatorname{lcm}(m, n) \iff k_p = \max(m_p, n_p)\text{，对所有}p$$

由此还可得一个小结论$n \cdot m = \gcd(m, n) \cdot \operatorname{lcm}(m, n)$

hdu4497 GCD and LCM

三个未知数x, y, z，它们的gcd为G，lcm为L，G和L已知，求(x, y, z)三元组的个数。

hdu4497 GCD and LCM

三个未知数x, y, z，它们的gcd为G，lcm为L，G和L已知，求(x, y, z)三元组的个数。

对于每个素因子单独处理。

三个未知数x, y, z，它们的gcd为G，lcm为L，G和L已知，求(x, y, z)三元组的个数。

对于每个素因子单独处理。

假设素因子为p，L分解式中p的指数为l，G分解式中p的指数为g，那么显然$l < g$时不可能存在满足条件的三元组，所以只需要讨论$l \geq g$的情况，对于单个p因子，问题转化成了求三个数x_1, y_1, z_1，满足$\min(x_1, y_1, z_1) = g$且$\max(x_1, y_1, z_1) = g$，这是一个排列组合问题，三元组x_1, y_1, z_1的种类数当$l = g$时只有1中，否则答案就是 $6(l - g)$。

hdu4497 GCD and LCM

三个未知数x, y, z，它们的gcd为G，lcm为L，G和L已知，求(x, y, z)三元组的个数。

对于每个素因子单独处理。

假设素因子为p ，L分解式中p的指数为l，G分解式中p的指数为g，那么显然$l < g$时不可能存在满足条件的三元组，所以只需要讨论$l \geq g$的情况，对于单个p因子，问题转化成了求三个数x_1, y_1, z_1，满足$\min(x_1, y_1, z_1) = g$且$\max(x_1, y_1, z_1) = g$，这是一个排列组合问题，三元组x_1, y_1, z_1的种类数当$l = g$时只有1中，否则答案就是 $6(l - g)$。

最后根据乘法原理将每个素因子对应的种类数相乘就是最后的答案了。

求解不定方程$ax + by = \gcd(a, b)$(假设$a \geq b$)

扩展欧几里得

求解不定方程$ax+by=\gcd(a,b)$(假设$a\geq b$)
当$b=0$时有$\gcd(a,b)=a$,此时$x=1,y=0$。

扩展欧几里得

求解不定方程$ax + by = \gcd(a, b)$(假设$a \geq b$)
当$b = 0$时有$\gcd(a, b) = a$,此时$x = 1, y = 0$。
当b不为0时,根据GCD递归定理$\gcd(a, b) = \gcd(b, a \bmod b)$
可得$ax + by = \gcd(a, b) = \gcd(b, a \bmod b) = bx' + (a \bmod b)y'$

扩展欧几里得

求解不定方程$ax + by = \gcd(a, b)$(假设$a \geq b$)

当$b = 0$时有$\gcd(a, b) = a$,此时$x = 1, y = 0$。

当b不为0时,根据GCD递归定理$\gcd(a, b) = \gcd(b, a \bmod b)$

可得$ax + by = \gcd(a, b) = \gcd(b, a \bmod b) = bx' + (a \bmod b)y'$

即$ax + by = bx' + (a \bmod b)y' = bx' + (a - b * \lfloor a/b \rfloor)y'$

移项得$ax + by = bx' + (a \bmod b)y' = ay' + b(x' - \lfloor a/b \rfloor y')$

扩展欧几里得

求解不定方程$ax+by=\gcd(a,b)$(假设$a \geq b$)

当$b=0$时有$\gcd(a,b)=a$,此时$x=1, y=0$。

当b不为0时,根据GCD递归定理$\gcd(a,b)=\gcd(b, a \bmod b)$

可得$ax+by=\gcd(a,b)=\gcd(b, a \bmod b)=bx'+(a \bmod b)y'$

即$ax+by=bx'+(a \bmod b)y'=bx'+(a-b*\lfloor a/b \rfloor)y'$

移项得$ax+by=bx'+(a \bmod b)y'=ay'+b(x'-\lfloor a/b \rfloor y')$

所以$x=y', y=x'-\lfloor a/b \rfloor y'$

求解不定方程$ax + by = \gcd(a, b)$(假设$a \geq b$)

当$b = 0$时有$\gcd(a, b) = a$,此时$x = 1, y = 0$。

当b不为0时,根据GCD递归定理$\gcd(a, b) = \gcd(b, a \bmod b)$

可得$ax + by = \gcd(a, b) = \gcd(b, a \bmod b) = bx' + (a \bmod b)y'$

即$ax + by = bx' + (a \bmod b)y' = bx' + (a - b * \lfloor a/b \rfloor)y'$

移项得$ax + by = bx' + (a \bmod b)y' = ay' + b(x' - \lfloor a/b \rfloor y')$

所以$x = y', y = x' - \lfloor a/b \rfloor y'$

设 (x_0, y_0) 是不定方程 $ax + by = m$ 的一组解, $(a, b) = g$,那么全部解为 $(x_0 + (b/g)t, y_0 - (a/g)t)$,其中 t 为所有整数。

NOIP2012 同余方程

求关于 x 的同余方程 $ax \equiv 1 \pmod{b}$的最小正整数解。

NOIP2012 同余方程

求关于 x 的同余方程 $ax \equiv 1 \pmod{b}$的最小正整数解。

$$ax + yb = 1$$

【poj1061】青蛙的约会

　　有两只青蛙，青蛙A和青蛙B，它们在一个首尾相接的数轴上。设青蛙A的出发点坐标是x，青蛙B的出发点坐标是y。青蛙A一次能跳m米，青蛙B一次能跳n米，两只青蛙跳一次所花费的时间相同。数轴总长L米。x, y, m, n, L都是整数。要求它们至少跳了几次以后才会碰面。

Input

输入只包括一行5个整数x, y, m, n, L，其中$x \neq y < 2000000000$，$0 < m, n < 2000000000$，$0 < L < 2100000000$。

Output

输出碰面所需要的跳跃次数，如果永远不可能碰面则输出一行”Impossible”

求解a：

$$x + am \equiv y + an \pmod{L}$$

它就等于

$$a(m-n) \equiv y - x \pmod{L}$$

把模去掉，就等于

$$a(m-n) + Lk = y - x$$

然后，用exgcd求

$$a(m-n) + Lk = gcd(m-n, L)$$

设$d = \gcd(m-n, L)$，$c = y - x$。

若$c \bmod d \neq 0$，则无解。

这样解出a后，最终答案就是：

$$(a \cdot \frac{c}{d}) \bmod \frac{L}{d}$$

【NOI2002】荒岛野人

一个岛是环状的，环上排列有 M 个洞穴，顺时针编号为1到 M ，有 N (不超过 15) 个野人，第 i 个野人一开始住在洞穴 C_i 中，每一年要顺时针迁移 P_i 个洞穴，走 L_i 年后就会死去。求满足在野人有生之年都不存在两个野人同住一个洞穴的情况下，最少的洞穴总数。保证 M 不超过 10^6 。

一个岛是环状的，环上排列有 M 个洞穴，顺时针编号为1到 M ，有 N (不超过 15) 个野人，第 i 个野人一开始住在洞穴 C_i 中，每一年要顺时针迁移 P_i 个洞穴，走 L_i 年后就会死去。求满足在野人有生之年都不存在两个野人同住一个洞穴的情况下，最少的洞穴总数。保证 M 不超过 10^6 。

答案不满足单调性，不能二分。我们只能从小到大枚举洞穴数 M ，检查其是否能满足条件，和上一题类似。

mod：同余关系

若两个整数a, b除以正整数m有相同的余数，那么称a, b对于模m同余，用式子表示为：

$$a \equiv b \pmod{m} \iff a \bmod m = b \bmod m$$

mod：同余关系

若两个整数a, b除以正整数m有相同的余数，那么称a, b对于模m同余，用式子表示为：

$$a \equiv b \pmod{m} \iff a \bmod m = b \bmod m$$

在不产生歧义的情况下，可以省略 $(\mathrm{mod}\ m)$。

我们可以用另一种方式来解读同余式：$a - b = mk$，k是整数，即$m \mid a - b$。

mod：同余关系

若两个整数a, b除以正整数m有相同的余数，那么称a, b对于模m同余，用式子表示为：

$a \equiv b \pmod{m} \iff a \bmod m = b \bmod m$

在不产生歧义的情况下，可以省略 $(\bmod\ m)$。

我们可以用另一种方式来解读同余式：$a - b = mk$，k是整数，即$m \mid a - b$。

同余是一个等价关系，它满足自反律$a \equiv a$，对称律$a \equiv b$，传递律$a \equiv b \equiv c \Rightarrow a \equiv c$，这些都很容易证明。

mod：同余关系

若两个整数a, b除以正整数m有相同的余数，那么称a, b对于模m同余，用式子表示为：

$a \equiv b \pmod{m} \iff a \bmod m = b \bmod m$

在不产生歧义的情况下，可以省略$\pmod{m}$。

我们可以用另一种方式来解读同余式：$a - b = mk$，k是整数，即$m \mid a - b$。

同余是一个等价关系，它满足自反律$a \equiv a$，对称律$a \equiv b$，传递律$a \equiv b \equiv c \Rightarrow a \equiv c$，这些都很容易证明。

此外，它还满足可加减性：若$a \equiv b$ 且 $c \equiv d$，那么$a \pm c \equiv b \pm d$。 可乘性：若$a \equiv b$ 且 $c \equiv d$，那么$ac \equiv bd$。

mod：同余关系

若两个整数a, b除以正整数m有相同的余数，那么称a, b对于模m同余，用式子表示为：

$a \equiv b \pmod{m} \iff a \bmod m = b \bmod m$

在不产生歧义的情况下，可以省略$\pmod{m}$。

我们可以用另一种方式来解读同余式：$a - b = mk$，k是整数，即$m \mid a - b$。

同余是一个等价关系，它满足自反律$a \equiv a$，对称律$a \equiv b$，传递律$a \equiv b \equiv c \Rightarrow a \equiv c$，这些都很容易证明。

此外，它还满足可加减性：若$a \equiv b$ 且 $c \equiv d$，那么$a \pm c \equiv b \pm d$。 可乘性：若$a \equiv b$ 且 $c \equiv d$，那么$ac \equiv bd$。

我们对方程所习惯做的大多数运算对同余式都可以运用。但要注意，除法运算是有条件的。

逆元

Definition

设正整数模 m，对于任意正整数 a 满足 $(a, m) = 1$，存在 b 满足 $ab \equiv 1 \pmod{m}$，称 b 为模 m 意义下 a 的逆元。

逆元

Definition

设正整数模 m，对于任意正整数 a 满足 $(a,m)=1$，存在 b 满足 $ab \equiv 1 \pmod{m}$，称 b 为模 m 意义下 a 的逆元。

求逆元只需要用扩展欧几里得解一个线性同余方程$ab+mt=1$即可，还可以用费马小定理或欧拉定理来求。

逆元

Definition

设正整数模 m，对于任意正整数 a 满足 $(a, m) = 1$，存在 b 满足 $ab \equiv 1 \pmod{m}$，称 b 为模 m 意义下 a 的逆元。

求逆元只需要用扩展欧几里得解一个线性同余方程$ab + mt = 1$即可，还可以用费马小定理或欧拉定理来求。

而a有逆元的充要条件是$(a, m) = 1$（方程有解）。

逆元

Definition

设正整数模 m，对于任意正整数 a 满足 $(a, m) = 1$，存在 b 满足 $ab \equiv 1 \pmod{m}$，称 b 为模 m 意义下 a 的逆元。

求逆元只需要用扩展欧几里得解一个线性同余方程$ab + mt = 1$即可，还可以用费马小定理或欧拉定理来求。

而a有逆元的充要条件是$(a, m) = 1$（方程有解）。

可以$O(n)$预处理1到n的逆元。

定义1．剩余类：把关于模m同余的数归于一类，每类称为一个模m的剩余类。即由关于模m同余的数组成的集合，每一个集合叫做关于模m的一个剩余类(又叫同余类)。共有m个剩余类。

定义1．剩余类：把关于模m同余的数归于一类，每类称为一个模m的剩余类。即由关于模m同余的数组成的集合，每一个集合叫做关于模m的一个剩余类(又叫同余类)。共有m个剩余类。

设K_r是余数为r的剩余类，

则$K_r = \{qm + r \mid q \in \mathbb{Z}\} = \{a \mid a \in \mathbb{Z}, a \equiv r \pmod{m}\}$。

定义1. 剩余类：把关于模m同余的数归于一类，每类称为一个模m的剩余类。即由关于模m同余的数组成的集合，每一个集合叫做关于模m的一个剩余类(又叫同余类)。共有m个剩余类。

设K_r是余数为r的剩余类，

则$K_r = \{qm + r \mid q \in \mathbb{Z}\} = \{a \mid a \in \mathbb{Z}, a \equiv r \pmod{m}\}$。

定义2. 完系：设$K_0, K_1 \cdots K_{m-1}$是模m的m个剩余类，从K_r中各取一数 a_r 作为代表，则这样的m个数 $a_0, a_1 \cdots a_{m-1}$ 称为模m的一个完全剩余系，简称m的完系。例如最小非负完全剩余系：$0, 1, 2, \cdots, m-1$

剩余类、完系及简系

定义1. 剩余类：把关于模m同余的数归于一类，每类称为一个模m的剩余类。即由关于模m同余的数组成的集合，每一个集合叫做关于模m的一个剩余类(又叫同余类)。共有m个剩余类。

设K_r是余数为r的剩余类，

则$K_r = \{qm + r \mid q \in \mathbb{Z}\} = \{a \mid a \in \mathbb{Z}, a \equiv r \pmod{m}\}$。

定义2. 完系：设$K_0, K_1 \cdots K_{m-1}$是模m的m个剩余类，从K_r中各取一数 a_r 作为代表，则这样的m个数 $a_0, a_1 \cdots a_{m-1}$ 称为模m的一个完全剩余系，简称m的完系。例如最小非负完全剩余系：$0, 1, 2, \cdots, m-1$

- m个整数构成模m的一完全剩余系 $\Longleftrightarrow$ 两两模m不同余。
- 设$(a, m) = 1, b \in \mathbb{Z}$，若$x_1, x_2, \cdots, x_m$是模$m$的一个完全剩余系，则$ax_1 + b, ax_2 + b, \cdots, ax_m + b$也是模$m$的一个完全剩余系；特别地，$m$个连续的整数构成模$m$的一个完系。

$f[0]=0$, 当$n>1$时，$f[n]=(f[n-1]+a) \bmod b$。
数列f的特征是什么？

费马小定理

Theorem

设p是一个素数，a 是一个整数且不是 p 的倍数，那么

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

费马小定理

Theorem

设p是一个素数，a 是一个整数且不是 p 的倍数，那么

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

注意到若有 $i \not\equiv j \pmod{p}$，那么有 $i \times a \not\equiv j \times a \pmod{p}$。

费马小定理

Theorem

设p是一个素数，a 是一个整数且不是 p 的倍数，那么

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

注意到若有 $i \not\equiv j \pmod p$，那么有 $i \times a \not\equiv j \times a \pmod p$。
所以$1 \times a, 2 \times a, \cdots, (p-1) \times a$构成模$p$的一个完全剩余系。

费马小定理

Theorem

设p是一个素数，a 是一个整数且不是 p 的倍数，那么

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

注意到若有 $i \not\equiv j \pmod{p}$，那么有 $i \times a \not\equiv j \times a \pmod{p}$。

所以$1 \times a, 2 \times a, \cdots, (p-1) \times a$构成模$p$的一个完全剩余系。

由完全剩余系的性质，

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

费马小定理

Theorem

设p是一个素数，a 是一个整数且不是 p 的倍数，那么

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

注意到若有 $i \not\equiv j \pmod p$，那么有 $i \times a \not\equiv j \times a \pmod p$。

所以$1 \times a, 2 \times a, \cdots, (p-1) \times a$构成模$p$的一个完全剩余系。

由完全剩余系的性质，

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

即$(p-1)! \equiv (p-1)! \times a^{p-1} \pmod p$

费马小定理

Theorem

设p是一个素数，a 是一个整数且不是 p 的倍数，那么

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

注意到若有 $i \not\equiv j \pmod{p}$，那么有 $i \times a \not\equiv j \times a \pmod{p}$。

所以$1 \times a, 2 \times a, \cdots, (p-1) \times a$构成模$p$的一个完全剩余系。

由完全剩余系的性质，

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

即$(p-1)! \equiv (p-1)! \times a^{p-1} \pmod{p}$

又 $\gcd((p-1)!, p) = 1$，故$a^{p-1} \equiv 1 \pmod{p}$。

素性测试

很遗憾，费马小定理的逆定理是不成立的。 对 $a = 2$，满足 $2^{n-1} \bmod n = 1$ 的非素数 n 是存在的，比如 $n = 341 = 11 \times 31$。

素性测试

很遗憾，费马小定理的逆定理是不成立的。对 $a=2$，满足 $2^{n-1} \bmod n = 1$ 的非素数 n 是存在的，比如 $n = 341 = 11 \times 31$。

Definition

对于整数 a，称满足 $a^{n-1} \bmod n = 1$ 的合数为以 a 为底的 **伪素数**。

素性测试

很遗憾，费马小定理的逆定理是不成立的。 对 $a = 2$，满足 $2^{n-1} \bmod n = 1$ 的非素数 n 是存在的，比如 $n = 341 = 11 \times 31$。

Definition

对于整数 a，称满足 $a^{n-1} \bmod n = 1$ 的合数为以 a 为底的 **伪素数**。

经测试，前 10 亿的自然数中，同时以 2 和 3 为底的伪素数有 1272 个。 我们用费马小定理验证素数的话，出错的概率大概只有 0.000025。可以制作一张伪素数表。

素性测试

很遗憾，费马小定理的逆定理是不成立的。 对 $a=2$，满足 $2^{n-1} \bmod n = 1$ 的非素数 n 是存在的，比如 $n = 341 = 11 \times 31$。

Definition

对于整数 a，称满足 $a^{n-1} \bmod n = 1$ 的合数为以 a 为底的 **伪素数**。

经测试，前 10 亿的自然数中，同时以 2 和 3 为底的伪素数有 1272 个。 我们用费马小定理验证素数的话，出错的概率大概只有 0.000025。可以制作一张伪素数表。

如果我们随机选取若干个小于待测整数的正整数作为底 a，然后用费马小定理来测试呢？

素性测试

很遗憾，费马小定理的逆定理是不成立的。 对 $a = 2$，满足 $2^{n-1} \bmod n = 1$ 的非素数 n 是存在的，比如 $n = 341 = 11 \times 31$。

Definition

对于整数 a，称满足 $a^{n-1} \bmod n = 1$ 的合数为以 a 为底的 **伪素数**。

经测试，前 10 亿的自然数中，同时以 2 和 3 为底的伪素数有 1272 个。 我们用费马小定理验证素数的话，出错的概率大概只有 0.000025。可以制作一张伪素数表。

如果我们随机选取若干个小于待测整数的正整数作为底 a，然后用费马小定理来测试呢？

存在无穷多个被称为Carmichael数的整数：对于任意与其互素的整数a算法的计算结果都是1。最小的五个Carmichael数是561、1105、1729、2465和2801。

Miller-Rabin素性测试

费马小定理的逆命题不成立，所以只能使用逆否命题。

Miller-Rabin素性测试

费马小定理的逆命题不成立，所以只能使用逆否命题。

Theorem (二次探测定理)

若p是素数，x是一个正整数，且 $x^2 \bmod p = 1$，那么 $x \equiv \pm 1 \pmod{p}$。

费马小定理的逆命题不成立，所以只能使用逆否命题。

Theorem (二次探测定理)

若p是素数，x是一个正整数，且 $x^2 \bmod p = 1$，那么 $x \equiv \pm 1 \pmod{p}$。

由$x^2 \bmod p = 1$即 $p \mid x^2 - 1$ 即 $p \mid (x+1)(x-1)$，由 p 是素数易证。

Miller-Rabin素性测试

费马小定理的逆命题不成立，所以只能使用逆否命题。

Theorem (二次探测定理)

若p是素数，x是一个正整数，且 $x^2 \bmod p = 1$，那么 $x \equiv \pm 1 \pmod{p}$。

由$x^2 \bmod p = 1$即 $p \mid x^2 - 1$ 即 $p \mid (x+1)(x-1)$，由 p 是素数易证。

设待测数为 n，取一个比 n 小的正整数 a，设 $n - 1 = d \times 2^r$，若 n 是素数，则要么$a^d \bmod n = 1$，要么存在一个 i，满足 $0 \le i < r$ 且 $a^{d \times 2^i} \bmod n = -1$。

Miller-Rabin素性测试

费马小定理的逆命题不成立，所以只能使用逆否命题。

Theorem (二次探测定理)

若p是素数，x是一个正整数，且 $x^2 \bmod p = 1$，那么 $x \equiv \pm 1 \pmod{p}$。

由$x^2 \bmod p = 1$即 $p \mid x^2 - 1$ 即 $p \mid (x+1)(x-1)$，由 p 是素数易证。

设待测数为 n，取一个比 n 小的正整数 a，设 $n - 1 = d \times 2^r$，若 n 是素数，则要么$a^d \bmod n = 1$，要么存在一个 i，满足 $0 \le i < r$ 且 $a^{d \times 2^i} \bmod n = -1$。

随机选取 k 个小于待测整数 n 的正整数作为底 a，用上面的结论来测 试。时间复杂度 $O(k \log^2 n)$。

中国剩余定理

在《孙子算经》中有这样一个问题：有物不知其数，三三数之剩二，五五数之剩三，七七数之剩二。问物几何?

中国剩余定理

在《孙子算经》中有这样一个问题：有物不知其数，三三数之剩二，五五数之剩三，七七数之剩二。问物几何?

《孙子歌诀》：三人同行七十稀，五树梅花廿一支，七子团圆正半月，除百零五使得知。

中国剩余定理

在《孙子算经》中有这样一个问题：有物不知其数，三三数之剩二，五五数之剩三，七七数之剩二。问物几何?

《孙子歌诀》：三人同行七十稀，五树梅花廿一支，七子团圆正半月，除百零五使得知。

Example

求解一元线性同余方程组：

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

当m_i两两互素时，是经典的中国剩余定理，百度百科有详细的介绍。

中国剩余定理 扩展

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$

中国剩余定理 扩展

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$

它等价于

$$x = a_1 + k_1 m_1$$
$$x = a_2 + k_2 m_2$$

中国剩余定理 扩展

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$

它等价于

$$x = a_1 + k_1 m_1$$
$$x = a_2 + k_2 m_2$$

联立两个方程

$$k_1 m_1 - k_2 m_2 = a_2 - a_1$$

中国剩余定理 扩展

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$

它等价于

$$x = a_1 + k_1 m_1$$
$$x = a_2 + k_2 m_2$$

联立两个方程

$$k_1 m_1 - k_2 m_2 = a_2 - a_1$$

据裴蜀定理，我们可以知道如果 $\gcd(m_1, m_2) \mid (a_2 - a_1)$ 那么这个方程就有整数解，否则它就不存在整数解。

中国剩余定理 扩展

$$k_1 = \frac{m_2}{g} t + k_1'$$
$$k_2 = \frac{m_1}{g} t + k_2'$$

$$
\begin{aligned}
k_1 &= \frac{m_2}{g} t + k_1' \\
k_2 &= \frac{m_1}{g} t + k_2'
\end{aligned}
$$

往回代入可得

$$
\begin{aligned}
x &= a_1 + k_1 m_1 \\
&= x_0 + \frac{m_1 m_2}{g} t \\
&= x_0 + \operatorname{lcm}(m_1, m_2) t
\end{aligned}
$$

中国剩余定理 扩展

$$
\begin{aligned}
k_1 &= \frac{m_2}{g} t + k_1' \\
k_2 &= \frac{m_1}{g} t + k_2'
\end{aligned}
$$

往回代入可得

$$
\begin{aligned}
x &= a_1 + k_1 m_1 \\
&= x_0 + \frac{m_1 m_2}{g} t \\
&= x_0 + \operatorname{lcm}(m_1, m_2) t
\end{aligned}
$$

这个解实际上等价于下面这个同余方程

$$
x \equiv x_0 \pmod{\operatorname{lcm}(m_1, m_2)}
$$

题目：

求

$$\sum_{i=1}^{n}\left\lfloor\frac{n}{i}\right\rfloor$$

$(1 \leqslant n \leqslant 10^9)$

对于n/i取整，一共约有$2\sqrt{n}$个结果。

对于$i \leqslant \sqrt{n}$，n/i有$\sqrt{n}$个结果。

对于$\sqrt{n} < i \leqslant n$，n/i的范围是$1 \leqslant n/i \leqslant \sqrt{n}$，至多有$\sqrt{n}$个结果。

题目：余数之和

输入n,k，计算$\sum_{i=1}^{n} k \mod i$的结果。

解法：

和上一个题问题类似，商至多有$2\sqrt{k}$种。又注意到对于商相同，余数是一个等差数列。

如果除数的范围是l到r，商为k，对答案的贡献是$(r-l+1)*k-a(l+r)(r-l+1)/2$。

题目：模积和

输入n,m，计算

$$\sum_{1\leqslant i\leqslant n}\sum_{1\leqslant j\leqslant m, j\neq i}(n \mod i)(m \mod j)$$

解法：

如果没有$i \neq j$这个条件。

那么后面可以用分配律拆成两部分，然后乘起来。

$\sum_{i=1}^{n} n \mod i$是可以很容易在$O(\sqrt{n})$的时间内计算。

现在要求$i \neq j$，很容易想到先计算出全部，然后减去$i = j$的部分。

那么考虑对于n/i和m/i结果都相同的一组，$n \mod i$和$m \mod i$有什么性质。

容易发现后面两个均为等差数列，用分配率和前n个自然数和，平方和的公式就可以在$O(1)$的时间计算了。

总时间复杂度$O(\sqrt{n}+\sqrt{m})$。

$$\sum_{i=1}^{n}\sum_{j=1 \wedge i \neq j}^{m}(n \ mod \ i)(m \ mod \ j)$$

$$=\sum_{i=1}^{n}\sum_{j=1}^{m}(n-\left\lfloor\frac{n}{i}\right\rfloor i)(m-\left\lfloor\frac{m}{j}\right\rfloor j)-\sum_{i=1}^{min(n,m)}(n-\left\lfloor\frac{n}{i}\right\rfloor i)(m-\left\lfloor\frac{m}{i}\right\rfloor i)$$

$$=\left(\sum_{i=1}^{n}(n-\left\lfloor\frac{n}{i}\right\rfloor i)\right)\left(\sum_{j=1}^{m}(m-\left\lfloor\frac{m}{j}\right\rfloor j)\right)$$

$$-\sum_{i=1}^{min(n,m)}\left(nm+\left\lfloor\frac{n}{i}\right\rfloor\left\lfloor\frac{m}{i}\right\rfloor i^2-(m\left\lfloor\frac{n}{i}\right\rfloor+n\left\lfloor\frac{m}{i}\right\rfloor)i\right)$$

数论函数

数论函数是定义在整数集合上的函数。

数论函数是定义在整数集合上的函数。

一些常见的数论函数：

$\sigma(n) = \sum_{d|n} d$ ，表示正整数 n 的正因子之和。

$d(n) = \sum_{d|n} 1$ ，表示正整数 n 的正因子个数。

数论函数

数论函数是定义在整数集合上的函数。

一些常见的数论函数：

$\sigma(n) = \sum_{d|n} d$ ，表示正整数 n 的正因子之和。

$d(n) = \sum_{d|n} 1$ ，表示正整数 n 的正因子个数。

$\varphi(n)$ 表示 1 至 n 中与 n 互素的整数个数，称作欧拉函数。

数论函数

数论函数是定义在整数集合上的函数。

一些常见的数论函数：

$\sigma(n) = \sum_{d|n} d$，表示正整数 n 的正因子之和。

$d(n) = \sum_{d|n} 1$，表示正整数 n 的正因子个数。

$\varphi(n)$ 表示 1 至 n 中与 n 互素的整数个数，称作欧拉函数。

数论函数 f 叫作是积性函数，如果对任意两个互素的正整数 n 和 m，均有 $f(nm) = f(n)f(m)$

数论函数

数论函数是定义在整数集合上的函数。

一些常见的数论函数：

$\sigma(n) = \sum_{d|n} d$ ，表示正整数 n 的正因子之和。

$d(n) = \sum_{d|n} 1$ ，表示正整数 n 的正因子个数。

$\varphi(n)$ 表示 1 至 n 中与 n 互素的整数个数，称作欧拉函数。

数论函数 f 叫作是积性函数，如果对任意两个互素的正整数 n 和 m，均有 $f(nm) = f(n)f(m)$

欧拉函数

考虑如何计算$\varphi(n)$。

欧拉函数

考虑如何计算$\varphi(n)$。

$\varphi(p^k) = p^k - p^{k-1} = (p-1)p^{k-1}$

欧拉函数

考虑如何计算$\varphi(n)$。

$\varphi(p^k) = p^k - p^{k-1} = (p-1)p^{k-1}$

$\varphi(n)$是积性函数，但不是完全积性函数。

欧拉函数

考虑如何计算$\varphi(n)$。

$\varphi(p^k) = p^k - p^{k-1} = (p-1)p^{k-1}$

$\varphi(n)$是积性函数，但不是完全积性函数。

一个有趣的结论： $\sum_{d|n} \varphi(d) = n$

欧拉函数

考虑如何计算$\varphi(n)$。

$\varphi(p^k) = p^k - p^{k-1} = (p-1)p^{k-1}$

$\varphi(n)$是积性函数，但不是完全积性函数。

一个有趣的结论：$\sum_{d|n} \varphi(d) = n$

考虑分母为n的真分数，和它们化成最简分数，可以说明这个结论。

欧拉函数

考虑如何计算$\varphi(n)$。

$\varphi(p^k) = p^k - p^{k-1} = (p-1)p^{k-1}$

$\varphi(n)$是积性函数，但不是完全积性函数。

一个有趣的结论： $\sum_{d|n} \varphi(d) = n$

考虑分母为n的真分数，和它们化成最简分数，可以说明这个结论。

Theorem (欧拉定理)

设 n 为正整数，a 是与 n 互素的整数，则 $a^{\varphi(n)} \equiv 1 \pmod{n}$

欧拉函数

考虑如何计算$\varphi(n)$。

$\varphi(p^k) = p^k - p^{k-1} = (p-1)p^{k-1}$

$\varphi(n)$是积性函数，但不是完全积性函数。

一个有趣的结论： $\sum_{d|n} \varphi(d) = n$

考虑分母为n的真分数，和它们化成最简分数，可以说明这个结论。

Theorem (欧拉定理)

设 n 为正整数，a 是与 n 互素的整数，则 $a^{\varphi(n)} \equiv 1 \pmod{n}$

欧拉定理的证明与费马小定理类似。

莫比乌斯函数

如下定义莫比乌斯函数μ。

莫比乌斯函数

如下定义莫比乌斯函数μ。

$$\mu(n) = \begin{cases} 1, n = 1 \\ (-1)^k, n = p_1 p_2 \cdots p_k, p_i\text{为互异素数} \\ 0, \text{otherwise} \end{cases}$$

莫比乌斯函数

如下定义莫比乌斯函数μ。

$$\mu(n) = \begin{cases} 1, n = 1 \\ (-1)^k, n = p_1 p_2 \cdots p_k, p_i\text{为互异素数} \\ 0, \text{otherwise} \end{cases}$$

可知当n有平方因子时$\mu(n) = 0$。

莫比乌斯函数

如下定义莫比乌斯函数μ。

$$\mu(n) = \begin{cases} 1, n = 1 \\ (-1)^k, n = p_1 p_2 \cdots p_k, p_i\text{为互异素数} \\ 0, \text{otherwise} \end{cases}$$

可知当n有平方因子时$\mu(n) = 0$。
莫比乌斯函数是积性函数，因此我们可以通过线性筛来计算。

莫比乌斯函数

如下定义莫比乌斯函数μ。

$$\mu(n)=\begin{cases}1, n=1\\ (-1)^k, n=p_1p_2\cdots p_k, p_i\text{为互异素数}\\ 0, \text{otherwise}\end{cases}$$

可知当n有平方因子时$\mu(n)=0$。

莫比乌斯函数是积性函数，因此我们可以通过线性筛来计算。

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

莫比乌斯函数

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

莫比乌斯函数

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

$n = 1$时显然。

莫比乌斯函数

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

$n = 1$时显然。

$n > 1$，设$n = p_1^{k_1} p_2^{k_2} p_3^{k_3} \cdots p_m^{k_m}$。

莫比乌斯函数

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

$n = 1$时显然。

$n > 1$，设$n = p_1^{k_1} p_2^{k_2} p_3^{k_3} \cdots p_m^{k_m}$。

显然d的每个质因子指数为1才有贡献，否则$\mu(d) = 0$。

莫比乌斯函数

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

$n = 1$时显然。

$n > 1$，设$n = p_1^{k_1} p_2^{k_2} p_3^{k_3} \cdots p_m^{k_m}$。

显然d的每个质因子指数为1才有贡献，否则$\mu(d) = 0$。

那么设d中有r个质因子。 $\mu(d) = (-1)^r$，这样的d有C_m^r个

莫比乌斯函数

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

$n = 1$时显然。

$n > 1$，设$n = p_1^{k_1} p_2^{k_2} p_3^{k_3} \cdots p_m^{k_m}$。

显然d的每个质因子指数为1才有贡献，否则$\mu(d) = 0$。

那么设d中有r个质因子。 $\mu(d) = (-1)^r$，这样的d有C_m^r个

所以

$$\sum_{d|n} \mu(d) = \sum_{r=0}^{m} (-1)^r C_m^r$$

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

$n = 1$时显然。

$n > 1$，设$n = p_1^{k_1} p_2^{k_2} p_3^{k_3} \cdots p_m^{k_m}$。

显然d的每个质因子指数为1才有贡献，否则$\mu(d) = 0$。

那么设d中有r个质因子。 $\mu(d) = (-1)^r$，这样的d有C_m^r个

所以

$$\sum_{d|n} \mu(d) = \sum_{r=0}^{m} (-1)^r C_m^r$$

我们有二项式定理

$$\sum_{r=0}^{m} (-1)^r C_m^r = \sum_{r=0}^{m} C_m^r (-1)^r 1^{m-r} = (-1+1)^m = 0$$

莫比乌斯反演

$$F(n)=\sum_{d|n} f(d) \iff f(n)=\sum_{d|n} \mu(d)F(\frac{n}{d})$$

$$F(n)=\sum_{n|d} f(d) \iff f(n)=\sum_{n|d} \mu(\frac{d}{n})F(d)$$

$$F(n)=\sum_{d|n} f(d) \iff f(n)=\sum_{d|n}\mu(d)F(\frac{n}{d})$$

$$F(n)=\sum_{n|d} f(d) \iff f(n)=\sum_{n|d}\mu(\frac{d}{n})F(d)$$

证明第一个：

$$\begin{aligned}
&\sum_{d|n}\mu(d)F(\frac{n}{d})\\
=&\sum_{d|n}\mu(d)\sum_{i|\frac{n}{d}} f(i)\\
=&\sum_{i|n} f(i)\sum_{d|\frac{n}{i}}\mu(d)\\
=&f(n)
\end{aligned}$$

关于gcd与数论函数的8题 传送门

$gcd(x,y)=1, 0\leq x,y\leq n$的对数。

关于gcd与数论函数的8题 传送门

$gcd(x, y) = 1, 0 \leq x, y \leq n$的对数。

$gcd(x, y) =$质数，$0 \leq x, y \leq n$的对数。

关于gcd与数论函数的8题 传送门

$gcd(x, y) = 1, 0 \leq x, y \leq n$的对数。

$gcd(x, y) =$质数，$0 \leq x, y \leq n$的对数。

$gcd(i, j, k) = 1, 0 \leq i, j, k \leq n$ 的个数。

关于gcd与数论函数的8题 传送门

$gcd(x,y)=1, 0\le x,y\le n$的对数。

$gcd(x,y)=$质数，$0\le x,y\le n$的对数。

$gcd(i,j,k)=1, 0\le i,j,k\le n$ 的个数。

$gcd(x,y)=d, 1<=x<=a, 1<=y<=b$的个数。多组数据

关于gcd与数论函数的8题 传送门

$gcd(x,y) = 1, 0 \leq x, y \leq n$的对数。

$gcd(x,y) =$质数，$0 \leq x, y \leq n$的对数。

$gcd(i,j,k) = 1, 0 \leq i,j,k \leq n$ 的个数。

$gcd(x,y) = d, 1 <= x <= a, 1 <= y <= b$的个数。多组数据

$gcd(x,y) = k, a <= x <= b, c <= y <= d$的个数。多组数据

关于gcd与数论函数的8题 传送门

$gcd(x, y) = 1, 0 \leq x, y \leq n$的对数。

$gcd(x, y) =$质数，$0 \leq x, y \leq n$的对数。

$gcd(i, j, k) = 1, 0 \leq i, j, k \leq n$ 的个数。

$gcd(x, y) = d, 1 <= x <= a, 1 <= y <= b$的个数。多组数据

$gcd(x, y) = k, a <= x <= b, c <= y <= d$的个数。多组数据

$gcd(x, y) =$质数，$0 \leq x, y \leq n$的对数。多组数据

关于gcd与数论函数的8题 传送门

$gcd(x, y) = 1, 0 \leq x, y \leq n$的对数。

$gcd(x, y) =$质数，$0 \leq x, y \leq n$的对数。

$gcd(i, j, k) = 1, 0 \leq i, j, k \leq n$ 的个数。

$gcd(x, y) = d, 1 <= x <= a, 1 <= y <= b$的个数。多组数据

$gcd(x, y) = k, a <= x <= b, c <= y <= d$的个数。多组数据

$gcd(x, y) =$质数，$0 \leq x, y \leq n$的对数。多组数据

$\sum_{1 \leq i \leq n} \mathrm{gcd}(i, n), n < 2^{32}$

关于gcd与数论函数的8题 传送门

$gcd(x, y) = 1, 0 \leq x, y \leq n$的对数。

$gcd(x, y) =$质数，$0 \leq x, y \leq n$的对数。

$gcd(i, j, k) = 1, 0 \leq i, j, k \leq n$ 的个数。

$gcd(x, y) = d, 1 <= x <= a, 1 <= y <= b$的个数。多组数据

$gcd(x, y) = k, a <= x <= b, c <= y <= d$的个数。多组数据

$gcd(x, y) =$质数，$0 \leq x, y \leq n$的对数。多组数据

$\sum_{1 \leq i \leq n} \mathrm{gcd}(i, n), n < 2^{32}$

数论十(一)题 传送门

NOI2010 能量采集

在平面直角坐标系中，点(x, y)的代价定义为它和原点的连线中经过多少的其他整点个数$\times 2+1$。求横坐标在1到n且纵坐标在1到m的所有点的代价和。 $n, m \leq 10^5$

NOI2010 能量采集

在平面直角坐标系中，点(x,y)的代价定义为它和原点的连线中经过多少的其他整点个数$\times 2+1$。求横坐标在1到n且纵坐标在1到m的所有点的代价和。 $n,m\le 10^5$

实际上要求：

$$\sum_{i=1}^{n}\sum_{j=1}^{m} gcd(i,j)$$

容斥或者莫比乌斯反演都行。

考虑方程$a^x = b \pmod p$

已知$a, b, p(2 \leqslant p \leqslant 10^9)$，其中$p$为质数。求$x$的最小正整数解。

Baby-step Gaint-step

解法

朴素的暴力显然是不可以的，注意到如果有解，那么一定满足$0 < x < p$。

设$t = \lfloor\sqrt{p}\rfloor, x = ct - d (0 \leqslant d < t)$。

于是有$(a^t)^c = ba^d \pmod p$。

注意到右边只有t个取值。可以先预处理出来。然后暴力枚举左边的c，直到左边的结果在右边出现。

原根和指数

Definition

设$(a,m)=1$，满足 $a^r \equiv 1 \pmod{m}$ 的最小正整数 r 叫作整数 a 模 m 的阶。

原根和指数

Definition

设$(a, m) = 1$，满足 $a^r \equiv 1 \pmod{m}$ 的最小正整数 r 叫作整数 a 模 m 的阶。

Theorem

设$(a, m) = 1$，r 为 a 模 m 的阶，则对每个正整数 k，$a^k \equiv 1 \pmod{m}$ 当且仅当 $r|k$。特别地，$r|\varphi(m)$。

原根和指数

Definition

设$(a, m) = 1$，满足 $a^r \equiv 1 \pmod{m}$ 的最小正整数 r 叫作整数 a 模 m 的阶。

Theorem

设$(a, m) = 1$，r 为 a 模 m 的阶，则对每个正整数 k，$a^k \equiv 1 \pmod{m}$ 当且仅当 $r | k$。特别地，$r | \varphi(m)$。

设$k = qr + s$，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 是满足 $a^r \equiv 1 \pmod{m}$ 的最小正整数，而 $0 \le s < r$，所以 $s = 0$。

原根和指数

Corollary

设$(a, m) = 1$，则 a 模 m 的阶是 r，当且仅当下列二条件成立：

- $a^r \equiv 1 \pmod{m}$。
- 对于 r 的每个素因子 p 有 $a^{r/p} \not\equiv 1 \pmod{m}$。

Corollary

设$(a, m) = 1$，则 a 模 m 的阶是 r，当且仅当下列二条件成立：

- $a^r \equiv 1 \pmod{m}$。
- 对于 r 的每个素因子 p 有 $a^{r/p} \not\equiv 1 \pmod{m}$。

若 a 模 m 的阶是 r，那么这两个条件显然成立。反之，设 l 为 a 模 m 的阶，由第一个条件知 $l|r$，若 $l \neq r$，则 $s = r/l > 1$，所以 s 有素因子 p，即 $s = pt$，于是 $r/p = lt$，而$a^{r/p} = (a^l)^t \equiv 1 \pmod{m}$，这就和第二个条件矛盾了。

原根和指数

Definition

若整数 a 模 m 的阶为 $\varphi(m)$，则 a 叫作是模 m 的原根。

原根和指数

Definition

若整数 a 模 m 的阶为 $\varphi(m)$，则 a 叫作是模 m 的原根。

Theorem

对于正整数 m，模 m 具有原根当且仅当 $m = 2, 4, p^a, 2p^a$，其中 p 是奇素数且$a \geq 1$。

原根和指数

Definition

若整数 a 模 m 的阶为 $\varphi(m)$，则 a 叫作是模 m 的原根。

Theorem

对于正整数 m，模 m 具有原根当且仅当 $m=2,4,p^a,2p^a$，其中 p 是奇素数且$a\geq 1$。

给出一个具有原根的模 m，找出任意一个原根。

因为原根通常都很小，所以从小往大枚举，用之前的推论来判定即可。

原根和指数

设模 m 有原根 g，则 $1, g, g^2, \cdots, g^{\varphi(m)-1}$ 为模 m 的缩系。所以对每个与 m 互素的整数 a，必存在惟一的整数 k，使得 $a \equiv g^k \pmod{m}$, $0 \le k \le \varphi(m) - 1$

设模 m 有原根 g，则 $1, g, g^2, \cdots, g^{\varphi(m)-1}$ 为模 m 的缩系。所以对每个与 m 互素的整数 a，必存在惟一的整数 k，使得 $a \equiv g^k \pmod{m}$, $0 \le k \le \varphi(m) - 1$

Definition

上述的 k 叫作 a（对于原根 g）模 m 的指数，表示成 $k = ind_g a$。指数也叫作离散对数。

设模 m 有原根 g，则 $1, g, g^2, \cdots, g^{\varphi(m)-1}$ 为模 m 的缩系。所以对每个与 m 互素的整数 a，必存在惟一的整数 k，使得 $a \equiv g^k \pmod{m}$, $0 \le k \le \varphi(m) - 1$

Definition

上述的 k 叫作 a（对于原根 g）模 m 的指数，表示成 $k = ind_g a$。指数也叫作离散对数。

设$(a, m) = (b, m) = 1$，则

- $a \equiv b \pmod{m}$ 当且仅当 $ind_g a = ind_g b$。
- $ind_g ab \equiv ind_g a + ind_g b \pmod{\varphi(m)}$。
- $ind_g a^n \equiv n \cdot ind_g a \pmod{\varphi(m)}$，$n$ 是整数。

原根和指数

给出三个正整数 p, k, a，其中 p 是质数，保证有解，输出所有满足 $x^k \equiv a \pmod{p}$ 且 $0 \le x \le p-1$ 的整数 x。

原根和指数

给出三个正整数 p, k, a，其中 p 是质数，保证有解，输出所有满足 $x^k \equiv a \pmod{p}$ 且 $0 \le x \le p-1$ 的整数 x。

第一步，找出模 p 的一个原根 g。

给出三个正整数 p, k, a，其中 p 是质数，保证有解，输出所有满足 $x^k \equiv a \pmod{p}$ 且 $0 \le x \le p-1$ 的整数 x。

第一步，找出模 p 的一个原根 g。

第二步，求出 $ind_g a$，设为 b，则有 $x^k \equiv g^b \pmod{p}$。

原根和指数

给出三个正整数 p, k, a，其中 p 是质数，保证有解，输出所有满足 $x^k \equiv a \pmod{p}$ 且 $0 \le x \le p-1$ 的整数 x。

第一步，找出模 p 的一个原根 g。

第二步，求出 $ind_g a$，设为 b，则有 $x^k \equiv g^b \pmod{p}$。

第三步，对同余式两边取离散对数有 $k \cdot ind_g x \equiv b \pmod{p-1}$。

给出三个正整数 p, k, a，其中 p 是质数，保证有解，输出所有满足 $x^k \equiv a \pmod{p}$ 且 $0 \leq x \leq p-1$ 的整数 x。

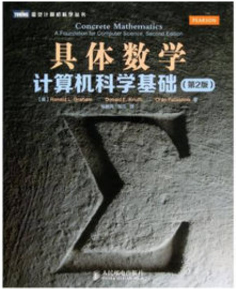
第一步，找出模 p 的一个原根 g。

第二步，求出 $ind_g a$，设为 b，则有 $x^k \equiv g^b \pmod{p}$。

第三步，对同余式两边取离散对数有 $k \cdot ind_g x \equiv b \pmod{p-1}$。

第四步，求解这个线性同余方程，找出所有解。

推荐图书



谢谢大家！