数论入门

VFleaKing

March 27, 2015

啦啦啦！大家好 vfk 又跟大家见面了！

今天我们要讲数论！是不是很激动呢！

我假设你们数论都只有小学水平啦！讲得都很水啦！欢迎睡觉呀！

推荐书籍《初等数论》（潘承洞和潘承彪写的那本），《具体数学》。

带余除法

设 a, b 都是整数，则存在唯一的一对整数 q 与 r 满足：

$$b = qa + r \qquad (0 \le r < |a|) \tag{1}$$

取整

$\lfloor x \rfloor$ 表示向下取整，$\lceil x \rceil$ 表示向上取整。

考虑带余除法 $b = qa + r$，容易知道 $q = \lfloor \frac{b}{a} \rfloor$。

坑爹：C++ 里 n / m 是按向零取整算的，你最好使用时 n, m 都别是负数。

取整的性质

- $\lfloor x + n \rfloor = ?$

取整的性质

- $\lfloor x + n \rfloor = ?$
- $\lfloor x + n \rfloor = \lfloor x \rfloor + n$

取整的性质

- $\lfloor x+n \rfloor = ?$
- $\lfloor x+n \rfloor = \lfloor x \rfloor + n$
- 用下取整符号表示上取整？

取整的性质

- $\lfloor x + n \rfloor = ?$
- $\lfloor x + n \rfloor = \lfloor x \rfloor + n$
- 用下取整符号表示上取整？
- $\lceil x \rceil = -\lfloor -x \rfloor$，$\lfloor x \rfloor = -\lceil -x \rceil$

取整的性质

- $\lfloor x + n \rfloor = ?$
- $\lfloor x + n \rfloor = \lfloor x \rfloor + n$
- 用下取整符号表示上取整？
- $\lceil x \rceil = -\lfloor -x \rfloor$，$\lfloor x \rfloor = -\lceil -x \rceil$
- 用 C++ 且不用浮点数算 $\lceil \frac{n}{m} \rceil$（$n, m \geq 0$）

取整的性质

- $\lfloor x + n \rfloor = ?$
- $\lfloor x + n \rfloor = \lfloor x \rfloor + n$
- 用下取整符号表示上取整？
- $\lceil x \rceil = -\lfloor -x \rfloor$，$\lfloor x \rfloor = -\lceil -x \rceil$
- 用 C++ 且不用浮点数算 $\lceil \frac{n}{m} \rceil$（$n, m \geq 0$）
- $\lceil \frac{n}{m} \rceil = \lfloor \frac{n+m-1}{m} \rfloor$
- 无论正负算 $\lfloor \frac{n}{m} \rfloor$ 技能 get！

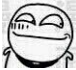
取整的性质

- $\lfloor x + n \rfloor = ?$
- $\lfloor x + n \rfloor = \lfloor x \rfloor + n$
- 用下取整符号表示上取整？
- $\lceil x \rceil = -\lfloor -x \rfloor$，$\lfloor x \rfloor = -\lceil -x \rceil$
- 用 C++ 且不用浮点数算 $\lceil \frac{n}{m} \rceil$（$n, m \geq 0$）
- $\lceil \frac{n}{m} \rceil = \lfloor \frac{n+m-1}{m} \rfloor$
- 无论正负算 $\lfloor \frac{n}{m} \rfloor$ 技能 get！
- 妈妈我要四舍五入！

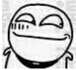
取整的性质

- $\lfloor x+n \rfloor = ?$
- $\lfloor x+n \rfloor = \lfloor x \rfloor + n$
- 用下取整符号表示上取整？
- $\lceil x \rceil = -\lfloor -x \rfloor$，$\lfloor x \rfloor = -\lceil -x \rceil$
- 用 C++ 且不用浮点数算 $\lceil \frac{n}{m} \rceil$（$n, m \geq 0$）
- $\lceil \frac{n}{m} \rceil = \lfloor \frac{n+m-1}{m} \rfloor$
- 无论正负算 $\lfloor \frac{n}{m} \rfloor$ 技能 get！
- 妈妈我要四舍五入！
- $\mathrm{round}(x) = \lfloor x + \frac{1}{2} \rfloor$

来纠结一下

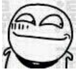
说从前有两个实数 α 和 β，还有个整数 n，满足 $\alpha \leq n \leq \beta$。然而作为全整数爱好者你不愿意存这两个实数，你想要给它加上某种取整符号存下来，该怎么办呢？

来纠结一下

说从前有两个实数 α 和 β，还有个整数 n，满足 $\alpha \le n \le \beta$。然而作为全整数爱好者你不愿意存这两个实数，你想要给它加上某种取整符号存下来，该怎么办呢？

答案：$\lceil \alpha \rceil \le n \le \lfloor \beta \rfloor$

来纠结一下

说从前有两个实数 α 和 β，还有个整数 n，满足 $\alpha \leq n \leq \beta$。然而作为全整数爱好者你不愿意存这两个实数，你想要给它加上某种取整符号存下来，该怎么办呢？

答案：$\lceil \alpha \rceil \leq n \leq \lfloor \beta \rfloor$

再来点东西纠结下吧：

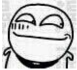
$$\alpha < n \iff \tag{2}$$

$$\alpha \leq n \iff \tag{3}$$

$$n < \beta \iff \tag{4}$$

$$n \leq \beta \iff \tag{5}$$

来纠结一下

说从前有两个实数 α 和 β，还有个整数 n，满足 $\alpha \le n \le \beta$。然而作为全整数爱好者你不愿意存这两个实数，你想要给它加上某种取整符号存下来，该怎么办呢？

答案：$\lceil \alpha \rceil \le n \le \lfloor \beta \rfloor$

再来点东西纠结下吧：

$$\begin{aligned}
\alpha < n &\iff \lfloor \alpha \rfloor < n && (2)\\
\alpha \le n &\iff \lceil \alpha \rceil \le n && (3)\\
n < \beta &\iff n < \lceil \beta \rceil && (4)\\
n \le \beta &\iff n \le \lfloor \beta \rfloor && (5)
\end{aligned}$$

继续来纠结一下

判断是否相等：

$$\left\lfloor \frac{x}{n} \right\rfloor \qquad \left\lfloor \frac{\lfloor x \rfloor}{n} \right\rfloor \tag{6}$$

$$\left\lfloor \frac{n}{x} \right\rfloor \qquad \left\lfloor \frac{n}{\lfloor x \rfloor} \right\rfloor \tag{7}$$

$$\left\lfloor \sqrt{x} \right\rfloor \qquad \left\lfloor \sqrt{\lfloor x \rfloor} \right\rfloor \tag{8}$$

继续来纠结一下

判断是否相等：

$$\left\lfloor \frac{x}{n} \right\rfloor = \left\lfloor \frac{\lfloor x \rfloor}{n} \right\rfloor \tag{6}$$

$$\left\lfloor \frac{n}{x} \right\rfloor \neq \left\lfloor \frac{n}{\lfloor x \rfloor} \right\rfloor \tag{7}$$

$$\left\lfloor \sqrt{x} \right\rfloor = \left\lfloor \sqrt{\lfloor x \rfloor} \right\rfloor \tag{8}$$

继续来纠结一下

判断是否相等：

$$\left\lfloor \frac{x}{n} \right\rfloor = \left\lfloor \frac{\lfloor x \rfloor}{n} \right\rfloor \tag{6}$$

$$\left\lfloor \frac{n}{x} \right\rfloor \neq \left\lfloor \frac{n}{\lfloor x \rfloor} \right\rfloor \tag{7}$$

$$\left\lfloor \sqrt{x} \right\rfloor = \left\lfloor \sqrt{\lfloor x \rfloor} \right\rfloor \tag{8}$$

如果一个连续函数 $f(x)$，当 x 不为整数时 $f(x)$ 一定不为整数，则对于任意 x 满足 $\lfloor f(x) \rfloor = \lfloor f(\lfloor x \rfloor) \rfloor$。

来做一道经典题冷静一下

给你 n，求：

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

$n \le 10^9$。

来做一道经典题冷静一下

给你 n，求：

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

$n \leq 10^9$。

做法：$k\left\lfloor \frac{n}{k} \right\rfloor \leq n$，总有一个 $\leq \sqrt{n}$，所以 $\left\lfloor \frac{n}{k} \right\rfloor \leq n$ 不超过 $2\sqrt{n}$ 个取值，所以分段搞搞。

取模

接下来来看带余除法 $b = aq + r$ 的另一部分：r。我们用 $b \bmod a$ 来表示 r，即：

$$n \bmod m = n - m\left\lfloor \frac{n}{m} \right\rfloor \tag{9}$$

坑爹：C++ 里由于 n / m 坑爹了，所以 n % m 也坑爹了。你最好使用时 n, m 都别是负数。

取模的性质

$$(a+b) \bmod m = (a \bmod m + b \bmod m) \bmod m \tag{10}$$

$$(a-b) \bmod m = (a \bmod m - b \bmod m) \bmod m \tag{11}$$

$$(a \times b) \bmod m = ((a \bmod m) \times (b \bmod m)) \bmod m \tag{12}$$

好吧其实都是废话。

取模的一个不是那么废话的性质

$$(cn) \bmod (cm) = \tag{13}$$

取模的一个不是那么废话的性质

$$(cn) \bmod (cm) = c(n \bmod m) \tag{13}$$

好吧其实也是废话。

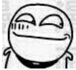
取模与 int

unsigned int 是对 2^{32} 取模哒！

而 int 仅仅只是把 $x \geq 2^{31}$ 的 x 看作了 $x - 2^{32}$ 而已，其实还是对 2^{32} 取模哒！

快速幂

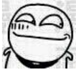
求 $a^b \bmod m$

NOIP 内容 

快速乘

求 $a \cdot b \bmod m$

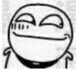
a, b, m 都是不超过 10^{18} 的 long long。

仿照快速幂，NOIP 内容 

快速乘

求 $a \cdot b \bmod m$

a, b, m 都是不超过 10^{18} 的 long long。

仿照快速幂，NOIP 内容 

人品算法：

```
(a * b - (long long) floor ((long double)a * b / m) * m + m) % m
```

爆零后果自负。

来做一道经典题冷静一下

给你 n，求：

$$\sum_{k=1}^{n} n \bmod k$$

$n \leq 10^9$。

来做一道经典题冷静一下

给你 n，求：

$$\sum_{k=1}^{n} n \bmod k$$

$n \leq 10^9$。

做法：按取模的定义式转换成前面那题。

来做一道毒瘤题冷静一下

来源：Codeforces Round #250 Div.1 D

维护有一个序列 $a_1, \ldots, a_n$，每次可以区间求和，单点赋值和区间取模。区间取模就是说给一个区间给一个 m，区间内元素都对 m 取模。

来做一道毒瘤题冷静一下

来源：Codeforces Round #250 Div.1 D

维护有一个序列 $a_1, \ldots, a_n$，每次可以区间求和，单点赋值和区间取模。区间取模就是说给一个区间给一个 m，区间内元素都对 m 取模。

做法：一个数被模一次会折半咯。

整除

设 a, b 都是整数且 $a \neq 0$，若存在整数 k 使得 $b = ak$，则称 $a \mid b$。

b 是 a 的倍数，a 就是 b 的约数啦。

公约数，公倍数

如果一个整数 d 满足 $d \mid a$ 且 $d \mid b$，则称 d 为 a 和 b 的公约数。

如果一个整数 d 满足 $a \mid d$ 且 $b \mid d$，则称 d 为 a 和 b 的公倍数。

啊这个定义可以拓展到任意多个数。

最大公约数，最小公倍数

a 和 b 的公约数中最大的那个，记为 $\gcd(a,b)$。

a 和 b 的公倍数中最小的那个，记为 $\mathrm{lcm}(a,b)$。

啊这个定义也可以拓展到任意多个数。

最大不仅仅是大小最大，还体现在公约数一定是最大公约数的约数。

最小不仅仅是大小最小，还体现在公倍数一定是最小公倍数的倍数。

求最大公约数

几千年前的业界毒瘤欧几里德倒腾出了辗转相除法。可是怎么证呢？

求最大公约数

几千年前的业界毒瘤欧几里德倒腾出了辗转相除法。可是怎么证呢？

注意到：

$$d \mid a, d \mid b \iff d \mid (a-b), d \mid b \tag{14}$$

公约数集合都是一样的，最大值能不相等吗？所以：

$$\gcd(a,b) = \gcd(a-b,b) = \gcd(a \bmod b, b) = \gcd(b, a \bmod b) \tag{15}$$

辗转相除法的时间复杂度

回忆刚才的毒瘤题，模一次折半嘛，显然是 $O(\log n)$ 的。

最坏情况是把相邻两个斐波拉契数列扔进去。

求最小公倍数

$\operatorname{lcm}(a, b)$ 可就没这么好的福气有个专门的算法咯，但是小学生都会做！

$$\operatorname{lcm}(a, b) = \frac{ab}{\gcd(a, b)} \tag{16}$$

来做一道经典题冷静一下

给你 a, b, c, n，求：

$$\sum_{x=1}^{n} \left\lfloor \frac{ax+b}{c} \right\rfloor$$

$a, b, c, n \leq 10^9$。

来做一道经典题冷静一下

给你 a, b, c, n，求：

$$\sum_{x=1}^{n} \left\lfloor \frac{ax+b}{c} \right\rfloor$$

$a, b, c, n \le 10^9$。

做法：辗转相除。

来做一道 BZOJ 权限题冷静一下

来源：BZOJ 2852 强大的区间

给你两个非负实数 a, b，求最小的 k 使得区间 (ka, kb) 中包含至少一个整数。

啊这个那个，a, b 整数部分不超过 $2^{31}-1$，小数部分不超过 300 位。（居然要开高精度超差评！）

来做一道 BZOJ 权限题冷静一下

来源：BZOJ 2852 强大的区间

给你两个非负实数 a, b，求最小的 k 使得区间 (ka, kb) 中包含至少一个整数。

啊这个那个，a, b 整数部分不超过 $2^{31}-1$，小数部分不超过 300 位。（居然要开高精度超差评！）

做法：辗转相除。最后高精度加减乘除取模被一网打进了……想练高精度的话推荐此题……

来做一道北京 WC2012 的题冷静一下

来源：BZOJ 2659 [Beijing wc2012] 算不出的算式

p, q 是两个奇素数，求：

$$\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor + \sum_{k=1}^{\frac{q-1}{2}} \left\lfloor \frac{kp}{q} \right\rfloor$$

来做一道北京 WC2012 的题冷静一下

来源：BZOJ 2659 [Beijing wc2012] 算不出的算式

p, q 是两个奇素数，求：

$$\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor + \sum_{k=1}^{\frac{q-1}{2}} \left\lfloor \frac{kp}{q} \right\rfloor$$

做法：$\frac{(p-1)(q-1)}{4}$，要特判 $p = q$ 的情况。

线性组合

整数 a, b 的线性组合是指形如 $sa + tb$ 的整数。其中 s, t 都是整数。

设所有 a, b 的线性组合组成的集合为 I，则 I 为所有 $\gcd(a, b)$ 的倍数构成的集合。怎么证呢？

线性组合

整数 a, b 的线性组合是指形如 $sa+tb$ 的整数。其中 s, t 都是整数。

设所有 a, b 的线性组合组成的集合为 I，则 I 为所有 $\gcd(a, b)$ 的倍数构成的集合。怎么证呢？

证明：拓展欧几里德给出了一个 $\gcd(a, b)$ 的构造，所以 $\gcd(a, b)$ 的倍数肯定在集合中。另一个方面，由于 $\gcd(a, b)$ 是 $sa+tb$ 的约数，所以线性组合一定是 $\gcd(a, b)$ 的倍数。

拓展欧几里德

NOIP 内容，大家都会，就不讲了。

素数

对于一个整数 n，称 $-n, -1, 1, n$ 为 n 的平凡约数，其它的约数称为非平凡约数。

如果一个不为 1 或 -1 的整数 p 没有非平凡约数，则称 p 为素数。

如果一个整数 n 有非平凡约数，则称 n 为合数。

然而我们一般为了方便把素数只限定在正整数。

算术基本定理

素因数分解是存在且唯一的。

证明思路之一是先通过线性组合证明对于素数 p，$p \mid ab$ 则 $p \mid a$ 或 $p \mid b$，然后就好证了。

《初等数论》上用三种思路证明了这个定理，不要不服。

小学生判素数，素因数分解，枚举约数

如果 $n = ab$ 则必有一个小于等于 $\sqrt{n}$，于是就可以 $O(\sqrt{n})$ 了。NOIP 内容，大家都会，就不讲了。

当然要是需要枚举每个约数，同样的道理我们枚举 1 到 $\sqrt{n}$ 的每个整数 d，如果 $d \mid n$ 的话就找到了两个约数 d 和 $\frac{n}{d}$。（注意特判 $d^2 = n$）

以素因数分解看问题

令 $a=\prod_k p_k^{\alpha_k}$，$b=\prod_k p_k^{\beta_k}$，则：

$$
\begin{aligned}
a \mid b &\iff \alpha_k \le \beta_k &(17)\\
ab &\iff \alpha_k + \beta_k &(18)\\
a/b &\iff \alpha_k - \beta_k &(19)\\
a \mid b &\iff \alpha_k \le \beta_k &(20)\\
\gcd(a,b) &\iff \min(\alpha_k,\beta_k) &(21)\\
\operatorname{lcm}(a,b) &\iff \max(\alpha_k,\beta_k) &(22)
\end{aligned}
$$

新高精度技能 get！普通的高精度算加减特别快，这种高精度算乘除特别快。

以素因数分解求组合数

给你 n, r, m，求：

$$\binom{n}{r} \bmod m$$

$n \leq 10^5, m \leq 10^9$。

以素因数分解求组合数

给你 n, r, m，求：

$$\binom{n}{r} \bmod m$$

$n \leq 10^5, m \leq 10^9$。

做法：裸上那个高精度。

来做一道搞笑题冷静一下

给你 p, r，其中 p 是素数，求：

$$\binom{p}{r} \bmod p$$

$p \leq 10^9$。

来做一道搞笑题冷静一下

给你 p, r，其中 p 是素数，求：

$$\binom{p}{r} \bmod p$$

$p \le 10^9$。

做法：$1 < r < p$ 时答案就是 0。

$n!$ 的素因数分解

$$n! = \prod_{k} p_k^{\alpha_k} \tag{23}$$

$$\alpha_k =$$

$n!$ 的素因数分解

$$n! = \prod_{k} p_k^{\alpha_k} \tag{23}$$

$$\alpha_k = \sum_{i \geq 1} \left\lfloor \frac{n}{p_k^i} \right\rfloor \tag{24}$$

来做一道经典题冷静一下

给你 n，求 $n!$ 的末尾有多少个 0。

来做一道经典题冷静一下

给你 n，求 $n!$ 的末尾有多少个 0。

做法：看 5 的个数。

素数的计数

素数会不会只有有限多个呢？

素数的计数

素数会不会只有有限多个呢？

欧几里德说：$\prod_{k=1}^{n} p_k + 1$。

素数定理

$\pi(x) \sim \frac{x}{\ln x}$

证明超级复杂！不要挣扎了！

我们 Oler 只用知道 $\pi(x) = O(\frac{x}{\log x})$ 就行了。

素数计数函数

$\pi(x)$ 表示 $\leq x$ 的素数的个数。

暴力：$O(n\sqrt{n})$

埃拉托斯特尼筛法：$O(n \log \log n)$

欧拉筛法：$O(n)$

欧拉筛法

让每个合数都被它的最小素因子筛去。

设一个合数 i 的最小素因子为 q_i。我们从小到大枚举 i，枚举到 i 时 1 到 i 的素数都已经被筛出，接着我们从小到大枚举不超过 q_i 的素数 p，把 $i \cdot p$ 标记为合数。

可不可以低于线性啊

当然可以！

用 p_i 表示从小到大第 i 个素数。

设 $f_m(n)$ 为 $1, \ldots, n$ 中不含 $p_1, \ldots, p_m$ 因子的数的个数。

$$f_m(n) = f_{m-1}(n) - f_{m-1}(\lfloor n/p_m \rfloor) \tag{25}$$

$f_m(n)$ 可以在 $O(m\sqrt{n})$ 的时间内求出。

现在我们选取一个 m 使得 $p_m^3 \geq n$，这就意味着 $f_m(n)$ 统计了两类数：一类是素数，另一类是两个大于 p_m 的素数乘起来得到的数。

第二类能在 $O(\sqrt{n} + \frac{n}{p_m})$ 时间内求出。由于 $m = \pi(n^{1/3}) = O(\frac{n^{1/3}}{\log n})$ 所以总时间复杂度 $O(\frac{n^{5/6}}{\log n})$。

可不可以更快一点啊

当然可以！

可不可以更快一点啊

当然可以！

把 m 搞成 $\pi(n^{1/4})$，最后就是要统计三类数：一类是素数，另一类是两个大于 p_m 的素数乘起来得到的数，另一类是三个大于 p_m 的素数乘起来得到的数。反正可以在 $O(\sqrt{n}+\frac{n}{p_m})$ 折腾出来，总时间复杂度 $O(\frac{n^{3/4}}{\log n})$

可不可以再快一点啊

你当跳蚤是香港记者啊说快就快啊……QAQ……自己去查论文吧。

啊给道裸题吧：Hackerrank Zenhacks Composite Numbers

同余

对于三个整数 a, b, m，如果满足 $m \mid (a - b)$ 则称 a 和 b 在模 m 的意义下同余。记作 $a \equiv b \pmod{m}$。

同余的性质

$a \equiv c \pmod{m}$，$b \equiv d \pmod{m}$，则：

$$a + c \equiv b + d \pmod{m} \tag{26}$$
$$a - c \equiv b - d \pmod{m} \tag{27}$$
$$ac \equiv bd \pmod{m} \tag{28}$$

除法

已知 a, b, m 和 $ax \equiv b \pmod{m}$，求 x。

除法

已知 a, b, m 和 $ax \equiv b \pmod{m}$，求 x。

等价于解 $ax + my = b$。所以 b 是 a, m 的一个线性组合，所以 $\gcd(a, m) \nmid b$ 时无解。只用考虑 $\gcd(a, m) \mid b$ 的情况。

除法

已知 a, b, m 和 $ax \equiv b \pmod{m}$，求 x。

等价于解 $ax + my = b$。所以 b 是 a, m 的一个线性组合，所以 $\gcd(a, m) \nmid b$ 时无解。只用考虑 $\gcd(a, m) \mid b$ 的情况。

由于性质：$ad \equiv bd \pmod{md} \iff a \equiv b \pmod{m}$，只用考虑 a 和 m 互质的情况。

除法

已知 a, b, m 和 $ax \equiv b \pmod{m}$，求 x。

等价于解 $ax + my = b$。所以 b 是 a, m 的一个线性组合，所以 $\gcd(a, m) \nmid b$ 时无解。只用考虑 $\gcd(a, m) \mid b$ 的情况。

由于性质：$ad \equiv bd \pmod{md} \iff a \equiv b \pmod{m}$，只用考虑 a 和 m 互质的情况。

然而还是不太好办，我们考虑更简单的情况：$b = 1$。

乘法逆元

（为啥要强调乘法！因为加法逆元是 $-x$）

已知 a, m 且 $\gcd(a, m) = 1$，$ax \equiv 1 \pmod{m}$，求 x。

乘法逆元

（为啥要强调乘法！因为加法逆元是 $-x$）

已知 a, m 且 $\gcd(a, m) = 1$，$ax \equiv 1 \pmod m$，求 x。

x 在模 m 意义下是存在且唯一的！存在性：拓展欧几里德。唯一性：如果有两组解 x_1, x_2，考虑 $x_1 a x_2 \bmod m$。

记 x 的逆元为 x^{-1}。

再战除法

再考虑 $ax \equiv b \pmod{m}$。对于 $\gcd(a, m) = 1$ 的情况。把两边同时乘以 a^{-1}，就可以解出 $x \equiv ba^{-1} \pmod{m}$。

结论：

再战除法

再考虑 $ax \equiv b \pmod{m}$。对于 $\gcd(a,m)=1$ 的情况。把两边同时乘以 a^{-1}，就可以解出 $x \equiv ba^{-1} \pmod{m}$。

结论：

- 当 $\gcd(a,m) \nmid b$ 时无解。

再战除法

再考虑 $ax \equiv b \pmod{m}$。对于 $\gcd(a, m) = 1$ 的情况。把两边同时乘以 a^{-1}，就可以解出 $x \equiv ba^{-1} \pmod{m}$。

结论：

- 当 $\gcd(a, m) \nmid b$ 时无解。
- 当 $\gcd(a, m) \mid b$ 时，$x \equiv ba^{-1} \pmod{\frac{m}{\gcd(a,m)}}$。其中 a^{-1} 是 a 在模 $\frac{m}{\gcd(a,m)}$ 意义下的逆元。

所以要是 $\gcd(a, m) \neq 1$ 你还想做除法就不要过多挣扎啦！

来做一道经典题冷静一下

给你 $p = 10^9 + 7$，多次询问，每次给你 n, r，快速求：

$$\binom{n}{r} \bmod p$$

$n, r \leq 10^5$。

来做一道经典题冷静一下

给你 $p = 10^9 + 7$，多次询问，每次给你 n, r，快速求：

$$\binom{n}{r} \bmod p$$

$n, r \le 10^5$。

做法：预处理阶乘和逆元就能做到每次 $O(1)$ 了。

预处理乘法逆元

拓展欧几里德每次求一次是 $O(\log n)$ 的。能不能再快一点啊！

如果我想一次性预处理出 $1, \ldots, n$ 的逆元，是可以再快的。

预处理乘法逆元

拓展欧几里德每次求一次是 $O(\log n)$ 的。能不能再快一点啊！

如果我想一次性预处理出 $1, \dots, n$ 的逆元，是可以再快的。

- 方法一：$(xy)^{-1} = x^{-1}y^{-1}$，我们可以在欧拉筛法的时候顺带求出逆元。我们用拓展欧几里德算 x 为素数的情况，总复杂度 $O(n + \frac{n}{\log n}\log n) = O(n)$

预处理乘法逆元

拓展欧几里德每次求一次是 $O(\log n)$ 的。能不能再快一点啊！

如果我想一次性预处理出 $1, \ldots, n$ 的逆元，是可以再快的。

- 方法一：$(xy)^{-1} = x^{-1}y^{-1}$，我们可以在欧拉筛法的时候顺带求出逆元。我们用拓展欧几里德算 x 为素数的情况，总复杂度 $O(n + \frac{n}{\log n}\log n) = O(n)$
- 方法二：先进行带余除法：$p = qx + r$。显然 $-r \equiv qx \pmod{p}$。然后两边同时除以 $-rx$ 则有：$x^{-1} \equiv -qr^{-1} \pmod{p}$。由于 $r < x$，我们就可以从小到大递推啦～

模多个数

$$x \equiv y \pmod{m_1} \tag{29}$$

$$x \equiv y \pmod{m_2} \tag{30}$$

求合体！

模多个数

$$x \equiv y \pmod{m_1} \tag{29}$$
$$x \equiv y \pmod{m_2} \tag{30}$$

求合体！

同余符号被扔进垃圾桶！$m_1 \mid (x-y)$，$m_2 \mid (x-y)$，所以可以得到：$\mathrm{lcm}(m_1, m_2) \mid (x-y)$。

$$x \equiv y \pmod{\mathrm{lcm}(m_1, m_2)} \tag{31}$$

可不可以再给力一点啊

有 n 个两两互质的正整数 $m_1, \ldots, m_n$，且：

$$x \equiv x_k \pmod{m_k} \tag{32}$$

求合体！

孙子定理（中国剩余定理）

x 在模 $\prod_k m_k$ 意义下是存在且唯一的。

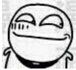
唯一性：刚刚的那个弱弱的合体就是证唯一性。

存在性：

$$x \equiv \sum_{k=1}^{n} M_k x_k M_k^{-1} \pmod{M} \tag{33}$$

M 是所有 m 之积，M_k 是除 m_k 以外的 m 之积，M_k^{-1} 是 M_k 在模 m_k 意义下的逆元。

类似物：拉格朗日插值法



来做一道 POI 题冷静一下

来源：POI 2008 Permutation

给你一个长度为 n 的序列 s，你把这个序列的所有不同排列按字典序排列后，求 s 的排名 $\bmod m$。

$n \le 300000, m \le 10^9$

来做一道 POI 题冷静一下

来源：POI 2008 Permutation

给你一个长度为 n 的序列 s，你把这个序列的所有不同排列按字典序排列后，求 s 的排名 $\bmod m$。

$n \leq 300000, m \leq 10^9$

做法：主要是除法太讨厌了，方法一是用前面说的奇葩高精度（只存 m 的素因子，另存一坨与 m 互质的部分），方法二是用中国剩余定理搞搞。

来做一道搞笑题冷静一下

给你 n, m，求：

$$n! \bmod m$$

$n \le 10^9, m \le 10^5$。

来做一道搞笑题冷静一下

给你 n, m，求：

$$n! \bmod m$$

$n \le 10^9, m \le 10^5$。

做法：

来做一道搞笑题冷静一下

给你 n，求：

$$(n-1)! \bmod n$$

$n \leq 10^9$。

来做一道搞笑题冷静一下

给你 n，求：

$$(n-1)! \bmod n$$

$n \le 10^9$。

做法：素数的话就把逆元配对，剩下 $x^2 \equiv 1 \pmod p$ 的即 $p \mid (x+1)(x-1)$，所以 $x \equiv \pm 1 \pmod p$，于是乘积就是 -1（嗯，这个叫威尔逊定理）。1 是 1，4 是 2，其它都是 0。

来做一道 trz 题冷静一下

来源：Codeforces Round #278 Div.1 C

给你 n，构造一个 1 到 n 的排列使得前缀积模 n 是 0 到 $n-1$ 的排列。无解输出“NO”

$n \leq 10^5$。

来做一道 trz 题冷静一下

来源：Codeforces Round #278 Div.1 C

给你 n，构造一个 1 到 n 的排列使得前缀积模 n 是 0 到 $n-1$ 的排列。无解输出 “NO”

$n \leq 10^5$。

做法：如果是不是 4 的合数那么中途一定会出现 0，所以一定无解。然后特判掉 1 和 4 只剩素数的情况，此时输出 $(x+1)x^{-1}$ 就行了。

费马小定理

对于一个素数 p 和一个不是 p 的倍数的 x，有：

$$x^{p-1} \equiv 1 \pmod{p} \tag{34}$$

费马小定理

对于一个素数 p 和一个不是 p 的倍数的 x，有：

$$x^{p-1} \equiv 1 \pmod p \tag{34}$$

证法一：$1, \ldots p-1$ 每个数乘以 x 再取模还是会得到原集合。

费马小定理

对于一个素数 p 和一个不是 p 的倍数的 x，有：

$$x^{p-1} \equiv 1 \pmod{p} \tag{34}$$

证法一：$1, \dots p-1$ 每个数乘以 x 再取模还是会得到原集合。

证法二：$(x+1)^p = x^p + 1 \pmod{p}$，然后按 x 大小归纳证。

快速幂求逆元

$$x^{-1} \equiv x^{p-2} \pmod{p} \tag{35}$$

欧拉定理

业界毒瘤欧拉把费马的结论加强了一下。

对于一个整数 m 和一个与 m 互质的 x，有：

$$x^{\varphi(m)} \equiv 1 \pmod{m} \tag{36}$$

其中 $\varphi(m)$ 表示 1 到 m 中与 m 互质的数的个数。

证明是显然的。

拉格朗日定理（群论）的推论

业界毒瘤拉格朗日给了个终极结论。

对于任意一个群 G，对于 G 中任意一个元素 x 有

$$x^{|G|} = 1 \tag{37}$$

（这只是推论。拉格朗日定理我们来日再侃）

来做一道 NOI 题冷静一下

来源：NOI 2013 矩阵游戏

$$F_{1,1} = 1 \tag{38}$$
$$F_{i,j} = a \times F_{i,j-1} + b \qquad j \neq 1 \tag{39}$$
$$F_{i,1} = c \times F_{i-1,m} + d \qquad i \neq 1 \tag{40}$$

求 $f_{n,m} \bmod (10^9+7)$。$n, m \leq 10^{1000000}$。

来做一道 NOI 题冷静一下

来源：NOI 2013 矩阵游戏

$$F_{1,1} = 1 \tag{38}$$
$$F_{i,j} = a \times F_{i,j-1} + b \qquad j \neq 1 \tag{39}$$
$$F_{i,1} = c \times F_{i-1,m} + d \qquad i \neq 1 \tag{40}$$

求 $f_{n,m} \bmod (10^9 + 7)$。$n, m \leq 10^{1000000}$。

做法：方法一是按十进制进行矩阵快速幂，方法二是解递推式然后变成求一个数的高精度次方，对 $p-1$ 取模即可。

欧拉定理能不能对任意 x 都成立呢？

$$x^{2\varphi(m)} \equiv x^{\varphi(m)} \pmod{m} \tag{41}$$

欧拉定理能不能对任意 x 都成立呢？

$$x^{2\varphi(m)} \equiv x^{\varphi(m)} \pmod{m} \tag{41}$$

证明：考虑 x 中与 m 公共的素因子和不公共的素因子。

推论：

$$x^n \equiv x^{\min\{n, n \bmod \varphi(m)+\varphi(m)\}} \pmod{m} \tag{42}$$

模素数意义下的多项式

回忆拉格朗日插值法，如果给你一个函数 $f:\{0,\ldots,p-1\}\mapsto\{0,\ldots,p-1\}$，我们一定能构造多项式 $\widehat{f}$ 满足对于任意 x:

$$\widehat{f}(x)\equiv f(x) \pmod p \tag{43}$$

所以多项式还是挺重要的！

实数域上多项式的零点

用 $\deg(f)$ 表示多项式 $f(x)$ 的次数。

对于多项式也是能玩带余除法的。$b(x) = q(x)a(x) + r(x)$，其中 $\deg(r) < \deg(a)$。

假设 $f(x_0) = 0$，让 $f(x)$ 对 $x - x_0$ 做带余除法，则有：

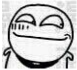
$$f(x) = q(x)(x - x_0) + r(x) \tag{44}$$

由于 $\deg(r) < 1$ 且 $r(x_0) = f(x_0) - q(x_0)(x - x_0) = 0$，所以 $r(x) = 0$。

易证对于 $x \neq x_0$ 时 $f(x) = 0 \iff q(x) = 0$，所以 $f(x)$ 的零点个数为 $q(x)$ 的零点个数加 1。

故实数域上的 n 次非零多项式有不超过 n 个根。

模素数意义下多项式的零点



拉格朗日定理（数论）

模 p 意义下 n 次非零多项式有不超过 $\min\{n, p\}$ 个根。

推论

实数域上两个 n 次多项式 f, g 如果有 $n+1$ 个 x 满足 $f(x)=g(x)$，那么这两个多项式相等。

模 p 意义下两个次数小于 p 的 n 次多项式 f, g 如果有 $n+1$ 个 x 满足 $f(x)=g(x)$，那么这两个多项式相等。

来做一道 NOIP 题冷静一下

来源：NOIP 2014 解方程

已知多项式方程：

$$a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n = 0$$

求这个方程在 $[1, m]$ 内的整数解（n 和 m 均为正整数）。

$0 < n \leq 100$，$|a_i| \leq 10^{10000}$，$a_n \neq 0$，$m \leq 1000000$。

来做一道 NOIP 题冷静一下

来源：NOIP 2014 解方程

已知多项式方程：

$$a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n = 0$$

求这个方程在 $[1, m]$ 内的整数解（n 和 m 均为正整数）。

$0 < n \leq 100$，$|a_i| \leq 10^{10000}$，$a_n \neq 0$，$m \leq 1000000$。

做法：先用一个小素数 p_s（机智地选取使得不为零多项式）得到 $n \cdot \frac{m}{p_s}$ 个根。然后再用大素数 p_b （机智地选取使得不为零多项式）判一遍得到 n 个根，再用压位了的高精度检验。记所有系数的十进制表示的最大长度为 l，时间复杂度 $O(nl + p_s n + n^2 \cdot \frac{m}{p_s} + nl)$，机智地选取 $p_s = O(\sqrt{nm})$ 则有 $O(nl + n\sqrt{nm})$。

来做一道经典题冷静一下

给你 p, d, n，其中 p 是素数，求：

$$\sum_{k=0}^{n} k^d$$

对 p 取模后的结果。

$p, n \leq 10^9$，$d \leq 10^5$。

来做一道经典题冷静一下

给你 p, d, n，其中 p 是素数，求：

$$\sum_{k=0}^{n} k^d$$

对 p 取模后的结果。

$p, n \leq 10^9$，$d \leq 10^5$。

做法：首先答案关于 n 肯定是个多项式，我们设为 $f(n)$。然后我们只要知道 $d+1$ 个 n 带入 f 后的取值后，就能把这个多项式通过插值求出来。所以无脑求出 $n = 0, \ldots, d$ 的结果，然后插值就行了。由于 n 是前几个自然数形式特殊，如果只需要求函数值不需要求系数是可以做到预处理 $O(d \log d)$ 求值一次 $O(d)$ 的。那个 $O(\log d)$ 是因为快速幂，利用欧拉筛法就能做到 $O(d)$ 了。

阶

对于两个互质的正整数 a, m，定义 a 对模 m 的阶为最小的正整数 d 满足：

$$a^d \equiv 1 \pmod{m} \tag{45}$$

记作 $\delta_m(a)$

阶的性质

- 有没有可能有 ρ 型循环?

阶的性质

- 有没有可能有 ρ 型循环?
- 一定是 O 型循环

阶的性质

- 有没有可能有 ρ 型循环？
- 一定是 O 型循环
- $\delta_m(a) \mid \varphi(m)$

阶的性质

- 有没有可能有 ρ 型循环？
- 一定是 O 型循环
- $\delta_m(a) \mid \varphi(m)$
- $\delta_m(a^k) = \frac{\delta_m(a)}{\gcd(\delta_m(a),k)}$

阶的性质

- 有没有可能有 ρ 型循环？
- 一定是 O 型循环
- $\delta_m(a) \mid \varphi(m)$
- $\delta_m(a^k) = \frac{\delta_m(a)}{\gcd(\delta_m(a),k)}$
- 推论：$\gcd(\delta_m(a), k) = 1$ 时，$\delta_m(a^k) = \delta_m(a)$

阶的性质

- 有没有可能有 ρ 型循环？
- 一定是 O 型循环
- $\delta_m(a) \mid \varphi(m)$
- $\delta_m(a^k) = \frac{\delta_m(a)}{\gcd(\delta_m(a),k)}$
- 推论：$\gcd(\delta_m(a), k) = 1$ 时，$\delta_m(a^k) = \delta_m(a)$

拉格朗日定理（群论）：嗨大家好，我们又见面了。我这里只是插播一句，对于任意一个群，$\delta(a)$ 是 $|G|$ 的约数。

求元素的阶

暴力枚举 $\varphi(m)$ 的约数。

原根

$\delta_m(g) = \varphi(m)$ 的整数 g 称为原根。

原根的次幂能恰好遍历所有 1 到 m 且与 m 互质的数。

求原根

如果有原根，那么肯定有 $\varphi(\varphi(m))$ 个，所以如果有原根的话，原根的数量是非常之多的。

暴力枚举几个或乱随机一通然后判定是否是原根就行啦！

判断一个数是不是原根其实也不用求元素的阶，只要枚举 $\varphi(m)$ 的素因子 p 然后判断 $g^{\varphi(m)/p} \equiv 1 \pmod{m}$ 是否成立，如果都不成立说明是原根。

求原根

如果有原根，那么肯定有 $\varphi(\varphi(m))$ 个，所以如果有原根的话，原根的数量是非常之多的。

暴力枚举几个或乱随机一通然后判定是否是原根就行啦！

判断一个数是不是原根其实也不用求元素的阶，只要枚举 $\varphi(m)$ 的素因子 p 然后判断 $g^{\varphi(m)/p} \equiv 1 \pmod{m}$ 是否成立，如果都不成立说明是原根。

请大家记住 998244353 的原根是 3，以后有大用途哟！

然而万一没有原根呢？

对于一个素数 p，是一定有原根的。

设 $\psi(d)$ 为 1 到 $p-1$ 中阶恰好为 d 的数的个数。对于一个 $p-1$ 的约数 n，方程 $x^n \equiv 1 \pmod p$ 一共有不超过 n 个解，于是有 $n \geq \sum_{d|n} \psi(d)$。用归纳法可证明 $\psi(d) = \varphi(d)$。

这里需要用到一个性质：

$$\sum_{d|n} \varphi(d) = n \tag{46}$$

考虑组合意义，$\varphi(d)$ 是与 n 的最大公约数为 $\frac{n}{d}$ 的数的个数。

有原根的家伙们

$$m = 1, 2, 4, p^\alpha, 2p^\alpha \tag{47}$$

其中 p 是奇素数。

证明过程比较感动，详见《初等数论》。

所以对于一些需要原根的问题但模数并没有原根，我们可以拆成若干个 p^α 分别解一下最后再用中国剩余定理合并一下。

但是 2^α 很讨厌。但是其实 2^α 还是有得救滴，可以证明 $\pm 5^k$ 能起到和原根类似的效果。

指标

若模 m 有原根 g，那么对于任意一个与 m 互质的整数 x，肯定存在某个 k 满足 $x \equiv g^k \pmod{m}$。

资瓷啊！非常资瓷啊！但是你把 k 求出来给我看看啊？

离散对数

对于整数 a, b, m，其中 a, b 均与 m 互质，定义 $\log_{m,b}(a)$ 为最小的整数 d 满足：

$$a^d \equiv b \pmod{m}$$

当然了，所有满足这个方程的整数 d 模 $\delta_m(a)$ 是同余的。

baby-step giant-step

设定一个参数 l。

首先求出 $a^0, a^1, \ldots, a^{l-1}$，存入一个哈希表。

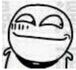
然后枚举 $k = 0, 1, \ldots, \left\lfloor \frac{\varphi(m)-1}{l} \right\rfloor$，判定是否存在 $0 \le j < l$ 满足 $a^{kl+j} \equiv b \pmod m$。

即判定是否存在 $0 \le j < l$ 满足 $a^j \equiv b \cdot a^{-kl} \pmod m$。

把 l 设为 $\sqrt{\varphi(m)}$，时间复杂度即为 $O(\sqrt{\varphi(m)})$。

不互质的情况

要是 a, b 不一定跟 m 互质呢？



欢迎去虐 BZOJ 3283 运算器第二问

来做一道 BZOJ 权限题冷静一下

来源：BZOJ 2219 数论之神

给你 n, a, m，其中 m 是奇数，求：

$$x^n \equiv a \pmod{m}$$

在 $[0, m)$ 中整数解的个数。

$n, a \le 10^9$，$d \le 5 \times 10^8$。

来做一道 BZOJ 权限题冷静一下

来源：BZOJ 2219 数论之神

给你 n, a, m，其中 m 是奇数，求：

$$x^n \equiv a \pmod{m}$$

在 $[0, m)$ 中整数解的个数。

$n, a \leq 10^9$，$d \leq 5 \times 10^8$。

做法：认真听课的同学都知道这没啥思维难度啦～为啥不出个 m 可能是偶数的情况给大家爽爽呢？

二次剩余

对于一个数 d 和一个奇素数 p，且 $p \nmid d$，若存在一个 x 满足 $x^2 \equiv d \pmod{m}$，则称 d 为模 p 意义下的二次剩余，否则称为二次非剩余。

欧拉判别法

对于一个奇素数 p 和 d，怎么判断 d 是不是模 p 意义下的二次剩余呢？

时间复杂度要求 $O(\log p)$ 怎么办呢？

欧拉判别法

对于一个奇素数 p 和 d，怎么判断 d 是不是模 p 意义下的二次剩余呢？

时间复杂度要求 $O(\log p)$ 怎么办呢？

关键是看指标的奇偶性。所以 $d^{\frac{p-1}{2}}$ 为 1 则为二次剩余，否则不是。咦，不是的话是多少呢？

欧拉判别法

对于一个奇素数 p 和 d，怎么判断 d 是不是模 p 意义下的二次剩余呢？

时间复杂度要求 $O(\log p)$ 怎么办呢？

关键是看指标的奇偶性。所以 $d^{\frac{p-1}{2}}$ 为 1 则为二次剩余，否则不是。咦，不是的话是多少呢？

设结果为 x，则 $x^2 \equiv 1 \pmod p$ 则 $x \equiv \pm 1 \pmod p$。所以不是的话算出来结果是 -1。

数论函数

刚才的一系列推导中，欧拉函数很抢镜头。那么接下来就来玩玩各种数论函数吧！

欧拉函数

$\varphi(n)$ 表示 1 到 n 中与 n 互质的数的个数。怎么求呢？

欧拉函数

$\varphi(n)$ 表示 1 到 n 中与 n 互质的数的个数。怎么求呢？

小学生容斥！假设 n 包含的素因子分别为 $p_1, \ldots, p_l$，那么就先拿出 n，减去含一个素数的，加上含两个素数的，减去含三个素数的……

欧拉函数

$\varphi(n)$ 表示 1 到 n 中与 n 互质的数的个数。怎么求呢？

小学生容斥！假设 n 包含的素因子分别为 $p_1, \ldots, p_l$，那么就先拿出 n，减去含一个素数的，加上含两个素数的，减去含三个素数的……

$$\varphi(n) = n \cdot \prod_k (1 - \frac{1}{p_k}) \tag{48}$$

欧拉函数

$\varphi(n)$ 表示 1 到 n 中与 n 互质的数的个数。怎么求呢？

小学生容斥！假设 n 包含的素因子分别为 $p_1, \ldots, p_l$，那么就先拿出 n，减去含一个素数的，加上含两个素数的，减去含三个素数的……

$$\varphi(n) = n \cdot \prod_k (1 - \frac{1}{p_k}) \tag{48}$$

可以用欧拉筛法 $O(n)$ 求 1 到 n 的数的欧拉函数值。

除数函数

$\tau(n)$ 表示 n 的正约数的个数。怎么求呢？

除数函数

$\tau(n)$ 表示 n 的正约数的个数。怎么求呢？

小学生都知道：

$$\tau(n) = \prod_k (1 + \alpha_k) \tag{49}$$

积性函数

如果一个数论函数 f 满足对于任意的互质正整数 n, m 均有 $f(nm) = f(n)f(m)$，则称为积性函数。

如果一个数论函数 f 满足对于任意的正整数 n, m 均有 $f(nm) = f(n)f(m)$，则称为完全积性函数。

比如 φ 和 τ 都是啦～

莫比乌斯变换

前面提到过，$\sum_{d|n}\varphi(d)$ 就是 n。在整除意义下，你要是做个前缀和啥的简直要人命，对所有约数求和才相当于加减法时的“前缀和”。

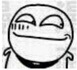
对于一个函数 g，我们定义它的莫比乌斯变换为 $f(n)=\sum_{d|n}g(d)$。莫比乌斯变换起到一种类似前缀和的作用。

来做一道水题冷静一下

给你 n 是奇数，求约数的约数个数之和。

来做一道水题冷静一下

给你 n 是奇数，求约数的约数个数之和。

做法：

莫比乌斯变换的积性

如果 g 是积性函数，那么对于互质的正整数 n, m:

$$\begin{aligned} f(nm) &= \sum_{d|nm} g(d) && (50) \\ &= \sum_{d_1|n}\sum_{d_2|m} g(d_1 d_2) && (51) \\ &= \sum_{d_1|n}\sum_{d_2|m} g(d_1)g(d_2) && (52) \\ &= \left(\sum_{d_1|n} g(d_1)\right)\left(\sum_{d_2|m} g(d_2)\right) && (53) \\ &= f(n)f(m) && (54) \end{aligned}$$

反之？

如果已知莫比乌斯变换，怎么求原函数呢？这个过程称为莫比乌斯反演。

当然了，如果是给一个数组要你做莫比乌斯变换，显然好搞，由于调和数神奇性质，就是 $O(n \log n)$ 了。给你一个数组做莫比乌斯反演，显然也好搞，只要倒过来写就行了。

如果是数学推导呢？

反之？

如果已知莫比乌斯变换，怎么求原函数呢？这个过程称为莫比乌斯反演。

当然了，如果是给一个数组要你做莫比乌斯变换，显然好搞，由于调和数神奇性质，就是 $O(n \log n)$ 了。给你一个数组做莫比乌斯反演，显然也好搞，只要倒过来写就行了。

如果是数学推导呢？

小学生容斥！假设 n 包含的素因子分别为 $p_1, \ldots, p_l$，那么就先拿出 $f(n)$，减去含一个素数的，加上含两个素数的，减去含三个素数的……

莫比乌斯函数

$$\mu(n) = \begin{cases} 1 & n = 1 \\ (-1)^r & n = \prod_{k=1}^{r} p_k \\ 0 & \end{cases} \tag{55}$$

那么莫比乌斯反演：

$$g(n) = \sum_{d|n} \mu(d) f(\frac{n}{d}) \tag{56}$$

狄利克雷卷积

由于下标不再是加减法，普通的卷积已经没啥价值了。

对于两个函数 f 和 g，它的狄利克雷卷积 h 为：

$$h(n) = \sum_{d|n} f(d)g(\frac{n}{d}) \tag{57}$$

记作 $f * g$。

易证 f 和 g 是积性函数则 $f * g$ 也是积性函数。

狄利克雷看莫比乌斯

$$f = g * (\lambda n : 1) \quad (58)$$

$$g = f * \mu \quad (59)$$

所以莫比乌斯变换为积性函数，则原函数为积性函数。

好用的莫比乌斯变换

$$\mu * (\lambda n : 1) = (\lambda n : [n = 1]) \tag{60}$$

$$\varphi * (\lambda n : 1) = (\lambda n : n) \tag{61}$$

$$\tag{62}$$

所以莫比乌斯变换为积性函数，则原函数为积性函数。

来做一道 SDOI 题冷静一下

来源：SDOI 2012 Longge 的问题

给定一个整数 n，求：

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

$n \leq 2^{32}$

来做一道 SDOI 题冷静一下

来源：SDOI 2012 Longge 的问题

给定一个整数 n，求：

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

$n \le 2^{32}$

做法：先证积性，再推素数的整数次幂的式子。

来做一道 NOI 题冷静一下

来源：NOI 2010 能量采集

给定两个整数 n，求：

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

$n, m \leq 10^5$

来做一道 NOI 题冷静一下

来源：NOI 2010 能量采集

给定两个整数 n，求：

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

$n, m \leq 10^5$

做法：莫比乌斯反演或欧拉函数直接搞。

来做一道 POI 题冷静一下

来源：POI 2007 Queries

多次询问，每次给定的整数 a, b, d，求有多少正整数对 x, y，满足 $x \le a, y \le b$，并且 $\gcd(x, y) = d$。

$a, b, d \le 50000$，询问次数不超过 50000。

来做一道 POI 题冷静一下

来源：POI 2007 Queries

多次询问，每次给定的整数 a, b, d，求有多少正整数对 x, y，满足 $x \le a, y \le b$，并且 $\gcd(x, y) = d$。

$a, b, d \le 50000$，询问次数不超过 50000。

做法：莫比乌斯反演或小学生容斥直接搞。用之前说的那个枚举 $\lfloor \frac{n}{i} \rfloor$ 的方法就能做到每次询问 $O(\sqrt{a} + \sqrt{b})$ 了。

来做一道 trz 题冷静一下

来源：UOJ Round #5 C

令 $p = 998244353$（$7 \times 17 \times 2^{23} + 1$，一个质数）。

给你整数 n, c, d。现在有整数 $x_1, \ldots, x_n$ 和 $b_1, \ldots, b_n$ 满足 $0 \le x_1, \ldots, x_n, b_1, \ldots, b_n < p$，且对于 $1 \le i \le n$ 满足：

$$\sum_{j=1}^{n} \gcd(i,j)^c \cdot \mathrm{lcm}(i,j)^d \cdot x_j \equiv b_i \pmod p \tag{63}$$

给出 $b_1, \ldots, b_n$，请你解出 $x_1, \ldots, x_n$ 的值。

$n \le 10^5$。

来做一道 trz 题冷静一下

来源：UOJ Round #5 C

令 $p = 998244353$（$7 \times 17 \times 2^{23} + 1$，一个质数）。

给你整数 n, c, d。现在有整数 $x_1, \ldots, x_n$ 和 $b_1, \ldots, b_n$ 满足 $0 \le x_1, \ldots, x_n, b_1, \ldots, b_n < p$，且对于 $1 \le i \le n$ 满足：

$$\sum_{j=1}^{n} \gcd(i,j)^c \cdot \operatorname{lcm}(i,j)^d \cdot x_j \equiv b_i \pmod p \tag{63}$$

给出 $b_1, \ldots, b_n$，请你解出 $x_1, \ldots, x_n$ 的值。

$n \le 10^5$。

做法：三次莫比乌斯反演。详见 UR #5 的题解。

各种基础技能 get

下面继续来搞点神奇的玩意儿玩玩。

再战判断素数

给一个整数 n，判断是否是素数。

$n \le 10^{18}$。

费马算法乱搞

随机几个不是 p 的倍数的 a 看是不是 $a^{p-1} \bmod p = 1$。

强伪素数打脸。

Miller-Rabin 算法

改进费马算法。

首先特判掉 2，然后碰到偶数直接说不是素数。

由于我们知道 $x^2 \equiv 1 \pmod{p}$ 只有两个根 ± 1。所以在快速幂的过程中，由于 $p-1$ 二进制末尾的一排 0 导致结果不断平方时，平方后如果是 1 那么平方前必须是 ± 1，否则就一定不是素数。

加了这个判断之后，对于所有的奇合数 n，在 $1, \ldots, n$ 中至少有 $\frac{3}{4}n$ 个 a 能证明 n 不是素数。随机选取 a 跑 k 次上述算法，就能做到 4^{-k} 的错误率。（你以为我会证？）

Miller-Rabin 掺了随机化，怎么种庄稼！

对于 $n \leq 10^{18}$，你把前 9 个素数作为 a 代入即可。

再战质因数分解

给一个整数 n，求质因数分解。

$n \leq 10^{18}$。

其实不如战这个问题

给一个整数 n，输出 n 的一个非平凡约数，或者弃疗。

Pollard-rho

生日悖论说，如果一年有 n 天，那么房间里有 $O(\sqrt{n})$ 个人的时候，有很大概率有两个人生日相同。

我们随手抓一个随机数递推序列例如 $x_k \equiv x_{k-1}^2 + c \pmod n$，这样有很大概率在 $\sqrt{n}$ 步内产生一个 ρ 型循环。

请注意，假设 n 的最小素因子为 p，那么模 p 意义下有很大概率在 $\sqrt{p}$ 步内产生一个 ρ 型循环。

假如在模 p 意义下产生了一个 ρ 型循环，$x_i \equiv x_j \pmod p$ 且 $x_i \not\equiv x_j \pmod n$，那么我们的机会就来了！求 $\gcd(n, x_i - x_j)$ 就行了！

所以我们计算 $x_1, x_2, \ldots$，计算到 x_i 时，设整数 k 满足 $2^k < i \leq 2^{k+1}$，我们求 $\gcd(n, x_i - x_{2^k})$ 看是不是非平凡约数就行了。一旦 x_{2^k} 是在模 p 意义下的环上，我们就能在约为环长的时间内找到 p 了。然而如果 $x_i = x_{2^k}$ 那么就说明模 n 意义下产生了一个环，这个时候可以重设随机函数再来一次。

我们可以先用 Miller-Rabin 判断 n 是否是素数，是的话就直接弃疗。

然后 n 现在是合数，我们能在 $O(\sqrt{p})$ 时间内找到 n 的一个非平凡约数。由于 $p \leq \sqrt{n}$，所以时间复杂度为 $O(n^{1/4})$。

写不死你烦死你系列

为了给 10^{18} 以内的整数 n 分解质因数，我们需要写 Miller-Rabin、Pollard-rho、快速乘、快速幂、gcd，祝你身体健康。

来做一道经典题冷静一下

给你 n，求大于等于 n 的最小素数。

$n \leq 10^{18}$。

来做一道经典题冷静一下

给你 n，求大于等于 n 的最小素数。

$n \le 10^{18}$。

做法：暴力枚举然后 Miller-Rabin 判断……素数是很稠密的，大概 $O(\log n)$ 就能碰到一个素数。

来做一道 BZOJ 权限题冷静一下

给定一个整数 n，求 n 最少可以拆成多少个完全平方数的和。

$n \le 10^{18}$。

来做一道 BZOJ 权限题冷静一下

给定一个整数 n，求 n 最少可以拆成多少个完全平方数的和。

$n \leq 10^{18}$。

做法：弃疗吧！不要尝试自己去推了！这是个结论题！（结论是什么以及怎么证见《初等数论》）反正最后要分解质因数的，当个模板题啥的也是极好的。

快速阶乘

给你 $n \le 10^9$ 和一个小素数，$n!$ 一定能写成 sp^α 的形式（$p \nmid s$），求 $s \bmod p$ 以及 α。

好吧其实一点都不快

把 1 到 n 中含因子 p 的数单独拎出来，那么就是要把 $\lfloor \frac{n}{p} \rfloor!$ 拆成 sp^{α} 形式再多乘上 $\lfloor \frac{n}{p} \rfloor$ 个 p。

然后剩下的数可以放心地对 p 取模，所以就是 $((p-1)!)^{\lfloor \frac{n}{p} \rfloor}(n \bmod p)!$。预处理 0 到 $p-1$ 的阶乘就好了。

注意每次 n 变为了 $\frac{n}{p}$，而 $(p-1)! \equiv -1 \pmod{p}$，所以不用写快速幂。

时间复杂度就是 $O(p \log n)$。

卢卡斯定理

由快速阶乘你可以推得“快速组合数”。

$$\binom{n}{r} \equiv \binom{n/p}{r/p}\binom{n \bmod p}{r \bmod p} \pmod{p} \tag{64}$$

不互质的时候

拆成 p^α 咯！然后瞎搞咯！最后中国剩余定理合并咯！就不赘述了。

给道题：SDOI2013 方程

再给道题：BZOJ 3283 运算器第三问

求组合数能不能再快一点啊

FFT 在路上等你。

完结撒花～

再次赞一下《初等数论》

以及欢迎围观《具体数学》

想要抽象的数论？比如在一般的交换环上发展数论？欢迎围观《抽象代数基础教程》。