数论常见结论及其证明

Qizy

2018 年 2 月 8 日

成都石室中学
yongzhengqi@gmail.com

目录

下取整函数的一条性质

结论

$\lfloor \frac{n}{d} \rfloor$ 至多只有 $2\sqrt{n}$ 种取值

证明

(α) $d \le \sqrt{n}$，有至多有 $\sqrt{n}$ 个 d，所以 $\lfloor \frac{n}{d} \rfloor$ 至多有 $\sqrt{n}$ 种不同的取值

(β) $d > \sqrt{n}$，有 $\lfloor \frac{n}{d} \rfloor < \sqrt{n}$，所以 $\lfloor \frac{n}{d} \rfloor$ 至多有 $\sqrt{n}$ 种不同的取值

由 $(\alpha), (\beta)$ 得 $\lfloor \frac{n}{d} \rfloor$ 至多只有 $2\sqrt{n}$ 种取值 $\square$

下取整函数的另一条性质

结论

若 $m \in \mathbb{Z}^+$，有：

$$\left\lfloor \frac{\lfloor x \rfloor}{m} \right\rfloor = \left\lfloor \frac{x}{m} \right\rfloor$$

证明

设 $\lfloor x \rfloor$ 存在分解 $qm + r$，其中 $q, r \in \mathbb{N}, r \in [0, m)$

$$LHS = \left\lfloor q + \frac{r}{m} \right\rfloor = q$$

$$RHS = \left\lfloor \frac{\lfloor x \rfloor}{m} + \frac{x - \lfloor x \rfloor}{m} \right\rfloor = \left\lfloor q + \frac{x - \lfloor x \rfloor + r}{m} \right\rfloor = q = LHS \qquad \square$$

欧拉函数的一条性质

结论

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

证明

考虑集合 $X_n = \{1, 2, 3, \ldots, n\}$。对于 $\forall m \in X_n$ 有唯一分解 $m = d \cdot \frac{m}{d}$ 满足 $d = (m, n)$

按 d 分类，构造集合 $A_i = \{d_i k \big| d_i \mid n, (k, \frac{n}{d_i} = 1), d_i k \leq n\}$，显然这些集合互不相交，又 $X_n = \bigcup A_i$，所以 $|X_n| = \sum |A_i|$

对于任意集合 A_i 有 $k = 1, 2, \cdots, \frac{n}{d_i}$，所以 $|A_i| = \frac{n}{d_i}$，所以 $|X_n| = n = \sum\limits_{d:d|n} \frac{n}{d}$ $\square$

σ_0 函数的一些性质

结论

$$\sigma_0(ab) = \sum_{i:i|a}\sum_{j:j|b}[\gcd(i,j)=1]$$

$$\sigma_0(abc) = \sum_{i:i|a}\sum_{j:j|b}\sum_{k:k|c}[\gcd(i,j)=\gcd(j,k)=\gcd(i,k)=1]$$

$$\dots$$

证明

按 $\gcd(a,b)$ 的不同质因子的个数 k 来归纳证明 $\sigma_0(ab)=\sum\limits_{i:i|a}\sum\limits_{j:j|b}[\gcd(i,j)=1]$：

(α) 当 $k=0$ 时，a,b 互质。因为 $\sigma_0(x)$ 是积性函数，所以 $\sigma_0(ab)=\sigma_0(a)\sigma_0(b)=(\sum\limits_{i:i|a}1)\cdot(\sum\limits_{j:j|b}1)=\sum\limits_{i:i|a}\sum\limits_{j:j|b}1=\sum\limits_{i:i|a}\sum\limits_{j:j|b}[\gcd(i,j)=1]$，即当 $k=0$ 时结论成立

(β) 当 $k\geq 1$ 时，取任意质因数 p，并将 a,b 分解：$a=Ap^{k_0},b=Bp^{k_1}$ 满足 $\gcd(A,p)=\gcd(B,p)=1$，有：

证明

$$
\begin{aligned}
\sigma_0(a,b) =&(k_0+k_1+1)\sigma_0(AB)\\
=&(k_0+k_1+1)\sum_{i:i|A}\sum_{j:j|B}[\gcd(i,j)=1] \qquad \text{（根据归纳假设）}\\
=&\sum_{i:i|Ap^{k_0}}\sum_{j:j|B}[\gcd(i,j)=1]+\sum_{i:i|A}\sum_{j:j|Bp^{k_1}}[\gcd(i,j)=1]\\
&-\sum_{i:i|A}\sum_{j:j|B}[\gcd(i,j)=1]\\
=&\sum_{i:i|Ap^{k_0}}\sum_{j:j|Bp^{k_1}}[\gcd(i,j)=1]\\
=&\sum_{i:i|a}\sum_{j:j|b}[\gcd(i,j)=1]
\end{aligned}
$$

所以在这种情况下，结论仍然成立

由 $(\alpha),(\beta)$ 得，$\sigma_0(ab)=\sum_{i:i|a}\sum_{j:j|b}[\gcd(i,j)=1]$ □

证明

$$\sigma_0(abc) = \sum_{i:i|a} \sum_{j:j|b} \sum_{k:k|c} [\gcd(i,j) = \gcd(j,k) = \gcd(i,k) = 1]$$ 的

证明：

`http://codeforces.com/blog/entry/5600`

欧拉定理的一个推论

结论

若 $x \geq \varphi(m)$，有：

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

证明

@beginendzrq 提供的证明：

`https://paste.ubuntu.com/26544742/`

除数函数的渐进上界

结论

在一定范围内，n 的约数至多有多少个呢？

10^5 以内 83160，128 个

10^6 以内 720720，240 个

10^7 以内 8648640，448 个

10^8 以内 73513440，768 个

10^9 以内 735134400，1344 个

int32 以内 2095133040，1600 个

10^{18} 以内 897612484786617600，103680 个

int64 以内 9200527969062830400，161280 个

参考资料

参考资料

金策. 数论函数及其求和

潘承洞, 潘承彪. 初等数论