数论讲义答案(第三章)

1. 证明: 若 n 为正整数, α为实数, 则

(1) $\left[\frac{[n\alpha]}{n}\right]=[\alpha]$,

(2) $[\alpha]+\left[\alpha+\frac{1}{n}\right]+\ldots+\left[\alpha+\frac{n-1}{n}\right]=[n\alpha]$.

证明:

(1) 设 $n\alpha = nq + r + \{n\alpha\}$, $0 \le r < n$, 则$[n\alpha] = nq + r$,

左边 $=\left[\frac{[n\alpha]}{n}\right]=\left[\frac{nq+r}{n}\right]=\left[q+\frac{r}{n}\right]=q$,

右边 $=[\alpha]=\left[\frac{n\alpha}{n}\right]=\left[\frac{nq+r+\{n\alpha\}}{n}\right]=\left[q+\frac{r+\{n\alpha\}}{n}\right]=q$

所以$\left[\frac{[n\alpha]}{n}\right]=[\alpha]$.

(2) 设 $n\alpha = nq + r + \{n\alpha\}$, $0 \le r < n$, 则$[n\alpha] = nq + r$, $\alpha = q +(r + \{n\alpha\})/n$.

$r = 0$ 时, $\alpha = q +\{n\alpha\}/n$, 左边 $= q + q + \ldots + q = nq$. 右边 $= nq$.

$r \ge 1$ 时, 左边 $=\left[q+\frac{r+\{n\alpha\}}{n}\right]+\left[q+\frac{r+\{n\alpha\}+1}{n}\right]+\ldots+\left[q+\frac{r+\{n\alpha\}+n-1}{n}\right]$

$$=nq+\sum_{k=0}^{n-r-1}\left[\frac{r+\{n\alpha\}+k}{n}\right]+\sum_{k=n-r}^{n-1}\left[\frac{r+\{n\alpha\}+k}{n}\right]$$

$$= nq + 0 + n - 1 - (n - r) + 1$$

$$= nq + r$$

$=[n\alpha]$ = 右边. #

2. 证明不等式

$$[2\alpha] + [2\beta] \ge [\alpha] + [\alpha + \beta] + [\beta]$$

证明:

设$\alpha = m + a$, $\beta = n + b$, $m, n\in Z$, $0 \le a, b < 1$. 不妨设 $a \ge b$, 则

$[2\alpha] + [2\beta] = [2m+2a] + [2n + 2b]$

$= 2m + 2n + [2a] + [2b]$

而

$$[\alpha] + [\alpha + \beta] + [\beta] = [m + a] + [n + b] + [m + n + a + b]$$
$$= 2m + 2n + [a] + [b] + [a+b]$$
$$= 2m + 2n + [a+b]$$

下证 $[2a] + [2b] \ge [a+b]$

而 $a \ge b$, 故$[2a]\ge[a+b]$,

自然有$[2a] + [2b] \ge [a+b]$. #

3. 证明: 若 $a > 0, b > 0, n > 0$, 满足 $n \mid a^n - b^n$, 则

$$n \mid (a^n - b^n)/(a-b).$$

证明:

设 $p^m \| n$, p 为一个素数, $a - b = t$, 若 $p \nmid t$, 则由 $p^m \mid a^n - b^n$, 自然有 $p^m \mid (a^n - b^n)/t$. 现设 $p \mid t$, 而

$$\frac{a^n - b^n}{t} = \frac{(b+t)^n - b^n}{t}$$

$$= \sum_{i=1}^{n} \binom{n}{i} b^{n-i} t^{i-1}$$

因为$\binom{n}{i} b^{n-i} t^{i-1} = n(n-1)\ldots(n-i+1) b^{n-i} \frac{t^{i-1}}{i!}$ (1)

在 $i = 1, 2, \ldots, n$ 时, $i!$中含 p 的最高方幂是

$$\sum_{k=1}^{\infty} \left[\frac{i}{p^k} \right] < \sum_{k=1}^{\infty} \frac{i}{p^k} = \frac{i}{p-1} \le i$$

又因 $p^{i-1} \mid t^{i-1}, p^m \mid n$, 故由(1)可知

$$p^m \mid \binom{n}{i} b^{n-i} t^{i-1},\ i = 1, \ldots, n.$$

即 $p^m \mid (a^n - b^n)/(a-b)$. 把 n 作因子分解并考察每一个素因子, 这就证明了 $n \mid (a^n - b^n)/(a-b)$.

#

4. 证明: 若 $n \ge 5, 2 \le b \le n$, 则

$$b-1 \left| \left[\frac{(n-1)!}{b}\right]\right. . \tag{1}$$

证明:

若 $b < n$, 则 $b(b-1) \mid (n-1)!$, 即 $b-1 \left| \left[\frac{(n-1)!}{b}\right]\right.$, 且 $\left[\frac{(n-1)!}{b}\right] \in Z$, 故(1)成立.

若 $b = n$, n 是一个合数且不是一个素数的平方, 可设 $b = n = rs$, $1 < r < s < n$, 由 $(n, n-1) = 1$ 知 $s < n-1$, 故 $b(b-1) = rs(n-1) \mid (n-1)!$, (1)式成立.

若 $b = n = p^2$, p 是一个素数, 由 $n = p^2 \ge 5$ 知, $1 < p < 2p < p^2 - 1 = n - 1$, 故 p, $2p$, $n - 1$ 是小于 n 的三个不同的数. 故 $p\cdot 2p\cdot(n-1) = 2b(b-1) \mid (n-1)!$, 故(1)式成立.

若 $b = n = p$, p 是一个素数, 由 $(p-1)! + 1 \equiv 0 \pmod p$知

$$\left[\frac{(p-1)!}{p}\right] = \left[\frac{(p-1)!+1}{p} - \frac{1}{p}\right] = \frac{(p-1)!+1}{p} - 1 = \frac{(p-1)!-(p-1)}{p}$$

即 $p\left[\frac{(p-1)!}{p}\right] = (p-1)!-(p-1)$, 而$(p, p-1) = 1$ 知$(p-1) \left| \left[\frac{(n-1)!}{p}\right]\right.$, (1)成立. #

5. 证明: 对于任意的正整数 n,

$$\frac{(2n)!}{n!(n+1)!}$$

是一个整数.

证明: 因为 $\mathrm{pot}_p((2n)!) = \sum_{i=1}^{\infty}\left[\frac{2n}{p^i}\right]$, $\mathrm{pot}_p((n)!) = \sum_{i=1}^{\infty}\left[\frac{n}{p^i}\right]$, $\mathrm{pot}_p((n+1)!) = \sum_{i=1}^{\infty}\left[\frac{n+1}{p^i}\right]$.

所以只需证

$$\forall\ i \ge 1,\ \left[\frac{2n}{p^i}\right] \ge \left[\frac{n}{p^i}\right] + \left[\frac{n+1}{p^i}\right]. \tag{*}$$

设 $n = qp^i + r$, $0 \le r < p^i$, 则若 $r < p^i - 1$, 则$\left[\frac{n+1}{p^i}\right] = q$, $\left[\frac{n}{p^i}\right] = q$, (*)式成立. 若 $r = p^i - 1$, 则$\left[\frac{n+1}{p^i}\right] = q+1$, $\left[\frac{n}{p^i}\right] = q$, 而

$$\left[\frac{2n}{p^i}\right]=\left[2q+\frac{2p^i-2}{p^i}\right]=\left[2q+1+\frac{p^i-1}{p^i}\right]\geq 2q+1=\left[\frac{n+1}{p^i}\right]+\left[\frac{n}{p^i}\right],$$

故此时(*)式也成立.

所以 $\frac{(2n)!}{n!(n+1)!}\in Z$. #

6. 证明: 设 $n=\sum_{j=1}^{k}n_j$, 则

(1) $\frac{n!}{n_1!n_2!\ldots n_k!}$ 是一个整数;

(2) 如 n 是一个素数, 而 $\max(n_1, \ldots, n_k) < n$, 则

$$n\mid\frac{n!}{n_1!n_2!\ldots n_k!}.$$

证明:

(1) 证法一 只需设 $n_1, n_2, \ldots, n_k$ 均为正数, 设 p 为任意素数, 则 $v_p((n)!)=\sum_{i=1}^{\infty}\left[\frac{n}{p^i}\right]$, $v_p((n_j)!)=\sum_{i=1}^{\infty}\left[\frac{n_j}{p^i}\right], 0\leq j\leq k$, 只需证 $\left[\frac{n_1+\ldots+n_k}{p^i}\right]\geq\sum_{j=1}^{k}\left[\frac{n_j}{p^i}\right]$ 对 $\forall i\geq 1$ 均成立, 而由 P64 性质 2 知这是显然的, 故 $\frac{n!}{n_1!n_2!\ldots n_k!}\in Z$.

证法二 $n=2$ 时, $\frac{n!}{n_1!(n-n_1)!}=\binom{n}{n_1}\in Z$,

假设 $n-1$ 时结论成立, 则当 n 时

$\frac{n!}{n_1!n_2!\ldots n_k!}=\frac{(n_1+n_2+\ldots+n_k)!}{n_1!n_2!\ldots n_k!}=\frac{(n_1+n_2)!}{n_1!n_2!}\frac{((n_1+n_2)+n_3+\ldots+n_k)!}{(n_1+n_2)!}\in Z$ (由归纳假设知 $\frac{((n_1+n_2)+n_3+\ldots+n_k)!}{(n_1+n_2)!}\in Z$, 又 $\frac{(n_1+n_2)!}{n_1!n_2!}\in Z$.)

(2) 若 n 是素数, 且 $\max(n_1, n_2, \ldots, n_k) < n$, 故 $n\mid n!$, 而 $n\nmid n_1!, n_2!, \ldots, n_k!$, 所以

$$n\mid\frac{n!}{n_1!n_2!\ldots n_k!}.$$ #

7. 证明: 如果在自然数列

$$1 \le a_1 < a_2 < \ldots < a_k \le n$$

中, 任意两个数 a_i, a_j 的最小公倍数$[a_i, a_j] > n$, 则 $k \le \left[\frac{n+1}{2}\right]$.

证明:

断言: 对于$\le 2n$ 的任意 $n+1$ 个正整数中, 至少有一个被另一个所整除.

设 $1 \le a_1 < a_2 < \ldots < a_{n+1} \le 2n$, $a_i = 2^{\lambda i} b_i$, $\lambda_i \ge 0$, $2 \nmid b_i$, $1 \le i \le n+1$, 其中 $b_i < 2n$. 因为在 $1, 2, \ldots, 2n$ 中只有 n 个不同的奇数 $1, 3, \ldots, 2n-1$, 故 $b_1, b_2, \ldots, b_{n+1}$ 中至少有两个相同. 设 $b_i = b_j$, $1 \le i < j \le n+1$, 于是在 $a_i = 2^{\lambda i} b_i$ 和 $a_j = 2^{\lambda j} b_i$ 中, 由 $a_i < a_j$ 知$\lambda_i < \lambda_j$. 故 $a_i \mid a_j$.

若 $k > \left[\frac{n+1}{2}\right]$. 当 $n = 2t$ 时, $k > \left[\frac{n+1}{2}\right] = t$, 故 $a_1, \ldots, a_k$ 为 $k(k \ge t+1)$个小于等于 $2t$ 的数, 故$\exists\, i, j$, $1 \le i < j \le k$, 使得 $a_i \mid a_j$. 故$[a_i, a_j] = a_j \le n$, 矛盾!

若 $n = 2t+1$, 则 $k > \left[\frac{n+1}{2}\right] = t+1$, 因为 $1, 2, \ldots, n = 2t+1$ 中只能有 $t+1$ 个奇数, 故 k 个数 $a_1, a_2, \ldots, a_k$ 中有一对数 i, j, $1 \le i < j \le k$, 使得 $a_i \mid a_j$, 所以 $[a_i, a_j] = a_j \le n$ 矛盾. 故 $k \le \left[\frac{n+1}{2}\right]$. #

8. 证明: 若 $k > 0$, 则

$$\sum_{\varphi(d)=k} u(d) = 0.$$

证明:

若$\exists\, d$, 使得$\varphi(d) = k$,

则(1) $2^2 \mid d$, 则 $u(d) = 0$ 不考虑.

(2) $2 \parallel d$, 则$(d/2, 2) = 1$, 所以$\varphi(d) = \varphi(2 \times d/2) = \varphi(2) \times \varphi(d/2) = \varphi(d/2) = k$.

而 $u(d) + u(d/2) = 0$.

(3) $2 \nmid d$, 则$\varphi(2d) = \varphi(2) \times \varphi(d) = \varphi(d) = k$, 而 $u(2d) + u(d) = 0$.

故$\{u(d) \ne 0 \mid u(d) = k\}$可分成若干对, 每对为 $u(d) + u(2d) = 0$. 故 $\sum_{\varphi(d)=k} u(d) = 0$. #

9. 证明

$$\sum_{d^2 \mid n} u(d) = u^2(n).$$

证明:

由 $u(n)$的定义有

$$u^2(n)=\begin{cases}1, & n\text{中不含有平方因子}\\ 0, & n\text{中含有平方因子}\end{cases},$$

当 n 中不含有平方因子时, 显然

$$\sum_{d^2|n}u(d)=u(1)=1$$

当 n 中含有平方因子时, 设 $n=n_0^2m, n_0>1, m$ 不含平方因子, 则

$$\sum_{d^2|n}u(d)=\sum_{d^2|n_0^2\cdot m}u(d)=\sum_{d^2|n_0^2}u(d)=\sum_{d|n_0>1}u(d)=0\,.$$

故

$$\sum_{d^2|n}u(d)=u^2(n). \qquad \#$$

其实, 采用类似的方法可证

$$\sum_{d^k|n}u(d)=\begin{cases}0, & \text{若 } m^k\mid n, m>1\\ 1, & \text{其它}\end{cases}.$$

10. 证明: 对于任一个素数 p,

$$\sum_{d|n}u(d)u((p,d))=\begin{cases}1, & \text{若 } n=1\\ 2, & \text{若 } n=p^\alpha, \alpha\ge 1\\ 0, & \text{若 } n\text{是其余情形}\end{cases}.$$

证明:

$n=1$ 结论显然.

若 $n=p^\alpha, \alpha\ge 1$, 则

$$\sum_{d|n}u(d)u((p,d))=u(1)u(1)+u(p)u(p)=2\,.$$

若$(n,p)=1$, 则

$$\sum_{d|n}u(d)u((p,d))=\sum_{d|n}u(d)=0\,.$$

若 $n=p^\alpha n_1, n_1>1$, 则

$$\sum_{d|n}u(d)u((p,d))=\sum_{\substack{d|n\\(d,p)=1}}u(d)+\sum_{\substack{d|n\\(d,p)=p}}u(d)u(p)=\sum_{d|n_1}u(d)+\sum_{d_1|n_1}u(d_1)u(p)=0 \qquad \#$$

11. 证明

$$\frac{n}{\varphi(n)}=\sum_{d|n}\frac{u^2(d)}{\varphi(d)}$$

证明:

$n=1$ 时结论显然.

$n>1$ 时，由于 $u(n)$, $\varphi(n)$ 均是积性函数，所以 $u^2(d)/\varphi(d)$, $\sum_{d|n}\frac{u^2(d)}{\varphi(d)}$ 也是积性函数. 设 $n=p_1^{\alpha 1}\ldots p_s^{\alpha s}$, 则

右边 $=\prod_{k=1}^{s}\left(1+\frac{u^2(p_k)}{\varphi(p_k)}+\ldots+\frac{u^2(p_k^{\alpha_k})}{\varphi(p_k^{\alpha_k})}\right)=\prod_{k=1}^{s}\left(1+\frac{1}{p_k-1}\right)=\prod_{k=1}^{s}\frac{p_k}{p_k-1}$.

左边 $=\frac{p_1^{\alpha_1}\ldots p_s^{\alpha_s}}{p_1^{\alpha_1-1}\ldots p_s^{\alpha_s-1}\prod_{k=1}^{s}(p_k-1)}=\frac{p_1\ldots p_s}{\prod_{k=1}^{s}(p_k-1)}=\prod_{k=1}^{s}\frac{p_k}{p_k-1}$.

故 $\sum_{d|n}\frac{u^2(d)}{\varphi(d)}=\frac{n}{\varphi(n)}$. #

12. 证明: $\sum_{d|n}u(d)\varphi(d)=0$ 的充分必要条件是 $n\equiv 0(\bmod\ 2)$.

证明:

设 $n=p_1^{\alpha_1}\ldots p_k^{\alpha_k}$, $p_1, \ldots, p_k$ 为不同的素数, $\alpha_i\geq 1$, $i=1, 2, \ldots, k$.

$$\sum_{d|n}u(d)\varphi(d)=u(1)\varphi(1)+\sum_{i=1}^{k}u(p_i)\varphi(p_i)+\ldots+u(p_1\ldots p_k)\varphi(p_1\ldots p_k)$$

$$=1+\sum_{i=1}^{k}(-1)(p_i-1)+\ldots+(-1)^k\prod_{i=1}^{k}(p_i-1)$$

$$=\prod_{i=1}^{k}(p_i-1-1)$$

所以, $\sum_{d|n}u(d)\varphi(d)=0\Leftrightarrow \exists$某个 $p_i=2\Leftrightarrow 2\mid n$. #

13. 证明:

$$\sum_{d=1}^{n}\varphi(d)\left[\frac{n}{d}\right]=\frac{n(n+1)}{2}(n>0).$$

证明:

$n=1$ 时结论显然.

假设对 $n=k$ 时成立，即

$$\sum_{d=1}^{k}\varphi(d)\left[\frac{k}{d}\right]=\frac{k(k+1)}{2}.$$

则 $n=k+1$ 时，有

$$\sum_{d=1}^{k+1}\varphi(d)\left[\frac{k+1}{d}\right]=\sum_{d=1}^{k}\varphi(d)\left[\frac{k}{d}\right]+\sum_{d=1}^{k}\varphi(d)\left(\left[\frac{k+1}{d}\right]-\left[\frac{k}{d}\right]\right)+\varphi(k+1)$$

$$=\frac{k(k+1)}{2}+\sum_{\substack{d\mid k+1\\ d<k+1}}\varphi(d)+\varphi(k+1)$$

$$=\frac{k(k+1)}{2}+\sum_{d\mid k+1}\varphi(d)$$

$$=\frac{k(k+1)}{2}+k+1$$

$$=\frac{(k+1)(k+2)}{2}.$$ #

证法二 因为 $\left[\frac{n}{d}\right]=\sum_{k=1}^{\left[\frac{n}{d}\right]}1$，所以

$$\sum_{d=1}^{n}\varphi(d)\left[\frac{n}{d}\right]=\sum_{d=1}^{n}\varphi(d)\sum_{k=1}^{\left[\frac{n}{d}\right]}1=\sum_{k=1}^{\left[\frac{n}{d}\right]}\sum_{d=1}^{n}\varphi(d)=\sum_{k=1}^{n}\sum_{d=1}^{\left[\frac{n}{k}\right]}\varphi(d)=\sum_{k=1}^{n}k\varphi(\left[\frac{n}{k}\right])=\sum_{k=1}^{n}\left[\frac{n}{k}\right]\varphi(k)$$

$$=n\varphi(1)+\left[\frac{n}{2}\right]\varphi(2)+\left[\frac{n}{3}\right]\varphi(3)+\ldots+\varphi(n)$$

$$=\sum_{d\mid 1}\varphi(d)+\sum_{d\mid 2}\varphi(d)+\ldots+\sum_{d\mid n}\varphi(d)$$

$$=1+2+\ldots+n$$

$$=\frac{n(n+1)}{2}.$$ #

14. 计算 $S(n)=\sum_{d\mid n}u(d)u\left(\frac{n}{d}\right)$.

解:

若 $n=1, S(1)=1$,

若 $n=p_1\ldots p_k$, 则

$$S(n)=\sum_{d\mid n}u(d)u\left(\frac{n}{d}\right)$$

$= u(1)u(p_1p_2\ldots p_k) + u(p_1)u(p_2\ldots p_k) + \ldots + u(p_k)u(p_1\ldots p_{k-1}) + \ldots + u(p_1p_2\ldots p_k)u(1)$

$= (-1)^k(C_k^0 + C_k^1 + \ldots + C_k^k)$

$= 2^k(-1)^k$

若 $n = p_1^2p_2\ldots p_k$，则

$$S(n) = \sum_{d|n} u(d)u\left(\frac{n}{d}\right) = u(p_1)u(p_1p_2\ldots p_k) = (-1)^{k+1}$$

其余情形 $S(n) = 0$. #

15. 证明: n 是素数的充分必要条件是$\sigma(n) + \varphi(n) = nd(n)$.

证明:

"$\Rightarrow$" 若 n 为素数，则 $\sigma(n) = 1 + n$，$\varphi(n) = n - 1$，$d(n) = 2$，所以有 $\sigma(n) + \varphi(n) = nd(n)$.

"$\Leftarrow$" n, $d(n)$, $\varphi(n)$, $\sigma(n)$均是极性函数，若 n 不为素数的方幂，$n = n_1n_2$，$(n_1, n_2) = 1$，

$$\begin{aligned}\sigma(n_1n_2) + \varphi(n_1n_2) &= \sigma(n_1)\sigma(n_2) + \varphi(n_1)\varphi(n_2)\\ &\neq (\sigma(n_1)+\varphi(n_1))\cdot(\sigma(n_2)+\varphi(n_2))\\ &= n_1n_2d(n_1n_2).\end{aligned}$$

若 $n = p^\alpha$，$\alpha \geq 1$，$\sigma(n) = 1 + p + \ldots + p^{\alpha-1} + p^\alpha$，$\varphi(n) = p^\alpha - p^{\alpha-1}$，$d(n) = \alpha + 1$，$1 + p + \ldots + p^{\alpha-2} + 2p^\alpha = (\alpha + 1)p^\alpha$，只有$\alpha = 1$时$\sigma(n) + \varphi(n) = nd(n)$才成立，即 n 是素数. #

16. 证明: 如果有正整数 n 满足

$$\varphi(n + 3) = \varphi(n) + 2, \tag{1}$$

则 $n = 2p^\alpha$ 或 $n + 3 = 2p^\alpha$，其中$\alpha \geq 1$, $p \equiv 3 \pmod 4$, p 是素数.

证明:

经验证可知 $n = 1, 2$ 不满足(1)式，设 $n > 2$，则$\varphi(n)$, $\varphi(n+3)$均为偶数. 由(1)知$\varphi(n)$和$\varphi(n+3)$不能同时被 4 整除，故只能有$\varphi(n) \equiv 2 \pmod 4$, $\varphi(n+3) \equiv 0 \pmod 4$或$\varphi(n) \equiv 0 \pmod 4$, $\varphi(n+3) \equiv 2 \pmod 4$.

令 $n = 2^{\alpha_1}p_2^{\alpha_2}\ldots p_k^{\alpha_k}$，则 $\varphi(n) = 2^{\alpha_1-1}p_2^{\alpha_2-1}(p_2-1)\ldots p_k^{\alpha_k-1}(p_k-1)$. 由于 $\varphi(n)$ 中 2^{α_1-1}, (p_2-1), …, (p_k-1)均被 2 整除，若$\varphi(n) \equiv 2 \pmod 4$，则 n 只能含有一个奇素数因子，因此 n 有三种情况: (1) $n = 2^{\alpha_1}$，此时$\alpha_1 = 2$，故 $n = 4$; (2) $n = p_2^{\alpha_2}$，此时 p_2

满足 $p_2 \equiv 3 \pmod 4$; (3) $n = 2^{\alpha_1}p_2^{\alpha_2}$, 此时$\alpha_1 = 1, p_2 \equiv 3 \pmod 4$, 即 $n = 2p_2^{\alpha_2}$. 因为$\varphi(4) \neq \varphi(1) + 2$, 所以若$\varphi(n+3) \equiv 2 \pmod 4$, 经类似的分析可得 $n + 3 = p^{\alpha}$, $2p^{\alpha}$, $\alpha \geq 1, p \equiv 3 \pmod 4$. 设 $n = p^{\alpha}$, 由(1)得

$$\varphi(p^{\alpha}+3) = p^{\alpha} - p^{\alpha-1} + 2 \tag{2}$$

设 $2^t \parallel p^{\alpha} + 3, t \geq 1$, 由(2)得

$$\begin{aligned} p^{\alpha} - p^{\alpha-1} + 2 &= \varphi(2^t \cdot (p^{\alpha} + 3)/2^t) \\ &= 2^{t-1} \cdot \varphi(\,(p^{\alpha} + 3)/2^t\,) \\ &\leq 2^{t-1} \cdot (\,(p^{\alpha} + 3)/2^t - 1) \\ &= (p^{\alpha} + 3)/2 - 2^{t-1} \end{aligned}$$

即有 $p^{\alpha} - p^{\alpha-1} + 2 \leq (p^{\alpha} + 3)/2 - 1$, 化简得 $p^{\alpha} \leq 2p^{\alpha-1} - 3$, 也即 $3 \leq p^{\alpha-1}(2-p)$
由于 $p > 2$, 故 $3 \leq p^{\alpha-1}(2-p)$不能成立. 同样可证 $n + 3 = p^{\alpha}$时, (1)式不成立, 故$n = 2p^{\alpha}$或 $n + 3 = 2p^{\alpha}$. #

17. 证明

$$\varphi(n) \geq n/d(n).$$

证明:

设 n 的标准分解式为 $n = p_1^{l_1} \dots p_s^{l_s}$, 故

$$\varphi(n)d(n) = n(1-1/p_1)\dots(1-1/p_s)(l_1 + 1)\dots(l_s + 1) \geq n(1/2)^s 2^s = n$$

于是得$\varphi(n) \geq n/d(n)$. #

18. 求出满足

$$\varphi(mn) = \varphi(m) + \varphi(n) \tag{1}$$

的全部正整数对(m, n).

解:

设$(m ,n) = d$, 则从$\varphi(n)$的公式不难有

$\varphi(mn) = d \cdot \varphi(m) \cdot \varphi(n)/\varphi(d)$,

由(1)得

$$\varphi(m) + \varphi(n) = d \cdot \varphi(m) \cdot \varphi(n)/\varphi(d), \tag{2}$$

设$\varphi(m)/\varphi(d) = a$, $\varphi(n)/\varphi(d) = b$, a, b 都是正整数, (2)化为

$$1/a + 1/b = d \tag{3}$$

$d > 2$ 时, 易证(3)无正整数解, 在 $d = 1$ 和 $d = 2$ 时, (3)分别仅有正整数解 $a = b = 2$

和 $a = b = 1$. 在 $d = 1$, $a = b = 2$ 时, $\varphi(m) = \varphi(n) = 2$, 因此$(m, n) = (3, 4), (4, 3)$; 在 $d = 2$, $a = b = 1$ 时, $\varphi(m) = \varphi(n) = 1$, 于是$(m, n) = (2, 2)$. #

19. 若 $n > 0$, 满足 $24 \mid n + 1$, 则 $24 \mid \sigma(n)$.

证明:

由 $24 \mid n + 1$ 知 $n \equiv -1 \pmod 3$和 $n \equiv -1 \pmod 8$, 设因子 $d \mid n$, 则 $3 \nmid d, 2 \nmid d$, 可设 $d \equiv 1, 2 \pmod 3$, $d \equiv 1, 3, 5, 7 \pmod 8$.

因为 $d\cdot(n/d) = n \equiv -1 \pmod 3$和 $d\cdot(n/d) = n \equiv -1 \pmod 8$, 由此推出,

$d \equiv 1 \pmod 3$, $n/d \equiv 2 \pmod 3$

或 $d \equiv 2 \pmod 3$, $n/d \equiv 1 \pmod 3$,

和 $d \equiv 3 \pmod 8$, $n/d \equiv 5 \pmod 8$

或 $d \equiv 5 \pmod 8$, $n/d \equiv 3 \pmod 8$

或 $d \equiv 1 \pmod 8$, $n/d \equiv 7 \pmod 8$

或 $d \equiv 7 \pmod 8$, $n/d \equiv 1 \pmod 8$.

每一种情形都有 $d + n/d \equiv 0 \pmod 3$, $d + n/d \equiv 0 \pmod 8$, 故 $d + n/d \equiv 0 \pmod{24}$. 又若 $d = n/d$, 则 $n = d^2$, $d > 1$, 则因为 $2 \nmid n$, 所以 $2 \nmid d$, 但 $n = d^2 \equiv 1 \pmod 8$矛盾. 所以 n 的所有正因子可以配对, 每对为 $d, n/d$, 故 $24 \mid \sigma(n)$. #

20. 证明: 若 $n = p_1^{\alpha 1} p_2^{\alpha 2} \cdots p_k^{\alpha k}$, $k \le 8$, 则$\varphi(n) > n/6$.

证明:

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\cdots\left(1 - \frac{1}{p_k}\right)$$

而 p_i 越大, $1 - 1/p_i$ 越大, 故只要证 $p_1, p_2, \ldots, p_8$ 为前 8 个素数时, $\varphi(n) > n/6$ 成立即可, 即要证$\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right)\cdots\left(1 - \frac{1}{19}\right) > \frac{1}{6}$, 而左边$=\frac{55296}{323323} > \frac{1}{6}$, 即结论成立. #

21. 设 $w(1) = 0$, $n > 1$, $w(n)$是 n 的不同的素因子的个数, 证明:

$$f(n) = w(n)*\mu(n) = 0 \text{ 或 } 1.$$

证明:

若 $n = p^{\alpha}\ (\alpha \ge 2)$

$$f(n) = w(n)*u(n) = \sum_{d \mid n} u(d)\, w\left(\frac{n}{d}\right) = u(1)\cdot w(p^{\alpha}) + u(p)\cdot w(p^{\alpha-1}) = u(1)\cdot 1 + (-1)\cdot 1 = 0.$$

若 $n=p$,

$$f(n)=w(n)*u(n)=w(1)\cdot u(p)+w(p)\cdot u(1)=1$$

若 $n=p_1^{\alpha 1}p_2^{\alpha 2}\cdots p_k^{\alpha k}, k\ge 2$, 则

$$
\begin{aligned}
f(n) &= w(n)*u(n) \\
&= \sum_{d|n} u(d)w\left(\frac{n}{d}\right) \\
&= C_k^0\cdot u(1)\cdot k + C_k^1\cdot u(-1)\cdot(k-1)+\ldots+C_k^{k-1}\cdot(-1)^{k-1}(k-(k-1))+C_k^k\cdot(-1)^k w(1) \\
&= ((x-1)^k)'|_{x=1} \\
&= 0
\end{aligned}
$$

#

22. 设 $f(x)$的定义域是[0, 1]中的有理数,

$$F(n)=\sum_{k=1}^{n} f\left(\tfrac{k}{n}\right),\ F^*(n)=\sum_{\substack{k=1\\(k,n)=1}}^{n} f\left(\tfrac{k}{n}\right),$$

证明: $F^*(n)=\mu(n)*F(n)$.

证明:

由 Mobius 变换定理知, 等价于证明 $F(n)=F^*(n)*e(n)$, 即要证

$$F(n)=\sum_{d|n}F^*(d)=\sum_{d|n}\sum_{\substack{k=1\\(k,d)=1}}^{d} f\left(\frac{k}{d}\right).$$

而对于 r/n, $r=1, 2, \ldots, n$ 的每个分数, 既约后均为 k/d, $d\mid n$, $k\le d$, $(k, d)=1$ 的形式, 即为某个 r/n, $1\le r\le n$. 故 $\sum_{d|n}\sum_{\substack{k=1\\(k,d)=1}}^{d} f\left(\frac{k}{d}\right)=\sum_{r=1}^{n} f\left(\frac{r}{n}\right)$, 即 $F(n)=\sum_{d|n}F^*(d)$, 再由 Mobius 逆变换即得. #

23. 证明: 若 $f(n)$是完全积性函数, 则对所有的数论函数 $g(n)$, $h(n)$, 有

$$f(n)\,(g(n)*h(n))=(f(n)g(n))*(f(n)h(n)).$$

证明:

$$
\begin{aligned}
f(n)\cdot(g(n)*h(n)) &= f(n)\cdot\left(\sum_{d|n} g(d)h\left(\frac{n}{d}\right)\right) \\
&= \sum_{d|n} f(n)g(d)h\left(\frac{n}{d}\right)
\end{aligned}
$$

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

$$= (f(n)\cdot g(n))*(f(n)\cdot h(n)) \qquad \#$$

24. 证明: 若$f(n)$和$f_1(n)$各为$g(n)$和$g_1(n)$的麦比乌斯变换, 则

$$\sum_{d|n} f(d)g_1\left(\tfrac{n}{d}\right) = \sum_{d|n} g(d)f_1\left(\tfrac{n}{d}\right).$$

证明:

$$f(n) = \sum_{d|n} g(d),\ f_1(n) = \sum_{d_1|n} g(d_1),$$

$$\sum_{d|n} f(d)g_1\left(\frac{n}{d}\right) = \sum_{d|n}\sum_{c|d} g(c)g_1\left(\frac{n}{d}\right)$$

$$\sum_{d|n} g(d)f_1\left(\frac{n}{d}\right) = \sum_{a|n}\sum_{b|\frac{n}{a}} g(a)g_1(b) = \sum_{b|\frac{n}{a}}\sum_{a|n} g(a)g_1(b)$$

令 $b = n/d$, 则$(n/d) \mid (n/a) \Rightarrow a \mid d$. 于是$\sum_{b|\frac{n}{a}}\sum_{a|n} g(a)g_1(b) = \sum_{d|n}\sum_{a|d} g(a)g_1\left(\frac{n}{d}\right)$.

故$\sum_{d|n}\sum_{c|d} g(c)g_1\left(\frac{n}{d}\right)$与$\sum_{a|n}\sum_{b|\frac{n}{a}} g(a)g_1(b)$展开式中每一项均相等, 因此

$$\sum_{d|n} f(d)g_1\left(\tfrac{n}{d}\right) = \sum_{d|n} g(d)f_1\left(\tfrac{n}{d}\right). \qquad \#$$

证法二 $f = g*e, f_1 = g_1*e$, 则$f*g_1 = g*e*g_1 = g*g_1*e = g*(g_1*e) = g*f_1$. #

25. 设$f(x)$是一个整系数多项式, $\psi(n)$代表

$$f(0), f(1), \cdots, f(n-1) \qquad (1)$$

中与 n 互素的数的个数, 证明:

(1) $\psi(n)$是积性数论函数;

(2) $\psi(p^{\alpha}) = p^{\alpha-1}(p-b_p)$, b_p 代表(1)中被素数 p 整除的数的个数.

证明:

(1) 需证 $\forall(m, n) = 1$,

$f(0)$, $f(1)$, …, $f(n-1)$

$f(n)$, $f(n+1)$, …, $f(2n-1)$

……

$f((m-1)\cdot n)$, $f((m-1)\cdot n+1)$, …, $f((m-1)\cdot n+n-1)$

中与 mn 互素的个数为 $\psi(m)\psi(n)$ 个.

又 $f(x)$ 为整系数多项式, 故

$f(i+n) \equiv f(i) \bmod n$

$f(i+m) \equiv f(i) \bmod m$

故上述 mn 个数中每一行与 n 互素的有 $\psi(n)$ 个, 所以 $f(0), f(1), \ldots, f((m-1)\cdot n+n-1)$ 中共有 $m\psi(n)$ 个与 n 互素的数. 而 $f(i)$, $f(n+i)$, …, $f((m-1)\cdot n+i)$ 由于 i, $n+i$, …, $(m-1)\cdot n+i$ 恰好通过 mod m 的一组完系, 所以上述 $m\psi(n)$ 个与 n 互素的数中有 $\psi(m)\psi(n)$ 个与 m 互素, 因此有 $\psi(mn) = \psi(m)\psi(n)$.

(2) $(a, p^{\alpha}) = 1 \Leftrightarrow (a, p) = 1$, 而

$$\begin{array}{llll} f(0), & f(1), & \ldots, & f(p-1) \\ f(p), & f(p+1), & \ldots, & f(2p-1) \end{array}$$

……

$f((p^{\alpha-1}-1)\cdot p)$, $f((p^{\alpha-1}-1)\cdot p+1)$, …, $f((p^{\alpha-1}-1)\cdot p+p-1)$

每一行与 p 互素个数为 $p-b_p$, 于是 $\psi(p^{\alpha}) = p^{\alpha-1}(p-b_p)$. #

26. 证明 $\sum\limits_{t|n}(d(t))^3 = (\sum\limits_{t|n}(d(t))^2$.

证明:

因为 d 为积性函数, 故 d^3, d^3*e, $(d*e)^2$ 均为积性函数, 故只需对 $n=1$ 及 $n=p^{\alpha}$ 证明上式即可!

$n=1$ 时, 左边 $=1=$ 右边, 故命题成立.

$n=p^{\alpha}$ 时, p 为素数, $\alpha \geq 1$ 时

$$\sum_{t|p^{\alpha}}(d(t))^3 = \sum_{i=0}^{\alpha}(d(p^i))^3 = \sum_{i=0}^{\alpha}(i+1)^3 = 1^3+2^3+\ldots+(\alpha+1)^3 = \frac{1}{4}(\alpha+1)^2(\alpha+2)^2$$

$$\left(\sum_{t|p^{\alpha}}d(t)\right)^2 = \left(\sum_{i=0}^{\alpha}d(p^i)\right)^2 = \left(\sum_{i=0}^{\alpha}(i+1)\right)^2 = \frac{1}{4}(\alpha+1)^2(\alpha+2)^2 = \sum_{t|p^{\alpha}}(d(t))^3. \quad \#$$

27. 找出所有的正整数 n 分别满足

(1) $\varphi(n) = n/2$; (2) $\varphi(n) = \varphi(2n)$; (3) $\varphi(n) = 12$.

证明: 设 $n = p_1^{\alpha 1} p_2^{\alpha 2}\cdots p_k^{\alpha k}$, $p_1 < p_2 < \ldots < p_k$, 则 $\varphi(n) = n(1-1/p_1)\ldots(1-1/p_k)$.

(1) 若 $\varphi(n) = n/2$, 则

$$(1-1/p_1)\ldots(1-1/p_k) = 1/2.$$

若 $t = 1$, 则 $p_1 = 2$, $n = 2^{\alpha}$即为所求.

若 $p_1 \neq 2$, $(1-1/p_1)\ldots(1-1/p_k) = 1/2$, 则 $2(p_1-1)\ldots(p_k-1) = p_1p_2\ldots p_k$, 而 $p_1, p_2, \ldots, p_k$ 均为不同的奇素数, 所以此时$\varphi(n) = n/2$ 不成立.

(2) 若 n 为奇数, $p_1, p_2, \ldots, p_k$ 均为不同的奇素数, 则

$$\varphi(2n) = 2n\left(1-\frac{1}{2}\right)\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_k}\right) = n\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_k}\right) = \varphi(n).$$

若 n 为偶数, 设 $p_1 = 2$, 则

$$\varphi(2n) = 2n\left(1-\frac{1}{2}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_t}\right) = 2n\left(1-\frac{1}{2}\right)\cdots\left(1-\frac{1}{p}\right) = 2\varphi(n).$$

所以当 n 是奇数时, $\varphi(n) = \varphi(2n)$.

(3) 若$\varphi(n) = p_1^{\alpha1-1}(p_1-1)\ p_2^{\alpha2-1}(p_2-1)\cdots\ p_k^{\alpha k-1}(p_k-1) = 12$, 则 $p_i - 1 \mid 12$, $i = 1, 2, \ldots, k$. 故 $p_i \in \{2, 3, 5, 7, 13\}$且 $k \leq 3$, $\alpha_i \leq 3$, $i = 1, 2, \ldots, k$. 则若 $2 \nmid n$, $\varphi(n) = 12$, 则 $n = 13, 3\times7$; 若 $2\|n$, 则 $n = 2\times13, 2\times3\times7$; 若 $4 \| n$, 则 $n = 4\times7$. 若 $2^k \| n$ $(k \geq 3)$, 则$\varphi(n) = \varphi(2^k)\cdot\varphi(n/2^k) = 2^{k-1}\cdot\varphi(n/2^k) = 12$ 没有整数解, 所以$\varphi(n) = 12$ 的解只有 $n = 13, 3\times7, 2\times13, 2\times3\times7, 4\times7$. #

28. 证明: 设 p_n 表示第 n 个素数, 则存在正常数 C_1, C_2 使

$$C_1\, n\log n < p_n < C_2\, n\log n.$$

证明:

$n \geq 2$ 时, 由第 7 节定理 1 有

$$\frac{1}{8}\frac{n}{\log n} \leq \pi(n) \leq 12\frac{n}{\log n}$$

将 n 换成 p_n, 有$\frac{1}{8}\frac{p_n}{\log p_n} \leq n \leq 12\frac{p_n}{\log p_n}$. (1)

上面不等式左边给出 $p_n \leq 8n\log p_n$. (2)

两边取对数有 $\log p_n \leq \log 8n + \log\log p_n$. (3)

又 $x > 1$ 时, $\log x < x/2$, 所以 $\log\log p_n < \log p_n/2$. 所以由(3)式, 有 $\log p_n/2<\log 8n$.

$\log p_n<2\log 8n\leq 8\log n$ (因为 $n \geq 2$, $(8n)^2 \leq n^8$)

再由(2)有, $p_n<64n\log n$, 取 $C_2 = 64$ 即可. 而(1)的右边给出 $p_n \geq n\log p_n/12> n\log n/12$, 故取 $C_1 = 1/12$ 即可. 即$(1/12)\, n\log n < p_n < 64\, n\log n$. #

29. 证明: 设 $f_1 = f_2 = 1, F_{n+2} = F_{n+1} + F_n (n \geq 0)$, 则

$$(F_m, F_n) = F_{(m,\, n)}.$$

证明:

(1) 首先证明对于 $n \geq 2, m \geq 1$ 有

$$f_{n+m} = f_{n-1}f_m + f_n f_{m+1}, \tag{*}$$

对 m 归纳证之

$m = 1$ 时, 要证 $f_{n+1} = f_{n-1}f_1 + f_n f_2 = f_{n-1} + f_n$ 即可.

假设小于 m 时(*)成立.

则等于 m 时, 由题设

$$\begin{aligned} f_{n+m} &= f_{n+m-1} + f_{n+m-2} \\ &= (f_{n-1}f_{m-1} + f_n f_m) + (f_{n-1}f_{m-2} + f_n f_{m-1}) \qquad \text{(归纳假设)} \\ &= f_{n-1}(f_{m-1} + f_{m-2}) + f_n(f_m + f_{m-1}) \\ &= f_{n-1} f_m + f_n f_{m+1} \quad (m \geq 3) \end{aligned}$$

$m = 2$ 时, $f_{n+2} = f_{n+1} + f_n = f_n + f_{n-1} + f_n = 2f_n + f_{n-1}f_2 = f_{n-1}f_2 + f_n f_3$

故(*)成立.

(2) 若 $m \mid n$, 则 $f_m \mid f_n$, 事实上, 设 $n = mn_1$, 对 n_1 归纳, $n_1 = 1$ 时显然, 设 $f_m \mid f_{mn_1}$, 则

$$f_{m(n_1+1)} = f_{mn_1+m} \overset{(1)}{=} f_{mn_1-1} \cdot f_m + f_{mn_1} \cdot f_{m+1}$$

故 $f_m \mid f_{m(n_1+1)}$

故 $m \mid n$ 时, $f_m \mid f_n$.

(3) $(f_n, f_{n+1}) = 1, n \geq 1$

设$(f_n, f_{n+1}) = d$, 则由题设 $f_{n+1} = f_n + f_{n-1} \Rightarrow d \mid f_{n-1}$, 继续下去得 $d \mid f_1 = 1$, 即 $d = 1$.

(4) 设 $m > n$, $(f_m, f_n) = f_{(m,\, n)}$. 若 $m = n$, 显然. 事实上, 设 $m = nq + r$, $0 < r < n$.(因若 $n \mid m$, 由(2)显然).

由(1)及(2)有:

$$\begin{aligned} (f_m, f_n) &= (f_{nq+r}, f_n) \\ &= (f_{nq-1}f_r + f_{nq}f_{r+1}, f_n) \\ &\overset{f_n \mid f_{nq}}{=} (f_{nq-1}f_r, f_n) \end{aligned}$$

而 $f_n \mid f_{nq}$, $(f_{nq-1}, f_{nq}) = 1$, $\therefore (f_{nq-1}, f_n) = 1$,

$\therefore (f_m, f_n) = (f_r, f_n)$

令 $n = q_1 r + r_0$, 同上又有$(f_r, f_n) = (f_r, f_{r_0}) = \ldots = f(m, n)$. #

30. 证明: 设 $f(n)$是一个积性函数, 则对素数的方幂 p^{α} $(\alpha \ge 1)$有

$$f(p^{\alpha}) = f(p)^{\alpha},$$

则 $f(n)$是完全积性函数.

证明:

设 $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, $n = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$, $\alpha_i \ge 0$, $\beta_i \ge 0$, $i = 1, 2, \ldots, k$.

$$f(m) = f(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}) = f(p_1^{\alpha_1}) \ldots f(p_k^{\alpha_k}) = f(p_1)^{\alpha_1} \ldots f(p_k)^{\alpha_k}.$$

同理, $f(n) = f(p_1)^{\beta_1} \ldots f(p_k)^{\beta_k}$. 所以

$$f(mn) = f(p_1^{\alpha_1+\beta_1} p_2^{\alpha_2+\beta_2} \cdots p_k^{\alpha_k+\beta_k}) = f(p_1)^{\alpha_1+\beta_1} \ldots f(p_k)^{\alpha_k+\beta_k}. \qquad \#$$

31. 证明: 若 $F(n), f(n)$是两个数论函数, 则 $F(n) = \prod_{d \mid n} f(d)$的充分必要条件是 $f(n) = \prod_{d \mid n} F(d)^{\mu(n/d)}$.

证明:

"⇒" $$\prod_{d \mid n} F(d)^{\mu(n/d)} = \prod_{d \mid n} \prod_{d_1 \mid d} f(d_1)^{\mu(n/d)}$$

$$= \prod_{d_1 \mid n} \prod_{t \mid (n/d_1)} f(d_1)^{\mu(n/td_1)} \qquad (d = d_1 t)$$

$$= \prod_{d_1 \mid n} f(d_1)^{\sum_{t \mid (n/d_1)} \mu(n/td_1)}$$

$$= \prod_{\substack{d_1 \mid n \\ n = d_1}} f(d_1)$$

$$= f(n)$$

"⇐" $$\prod_{d \mid n} f(d)^{\mu(n/d)} = \prod_{d \mid n} \prod_{d_1 \mid d} F(d_1)^{\mu(n/d)}$$

$$= \prod_{d_1 \mid n} \prod_{t \mid (n/d_1)} F(d_1)^{\mu(n/td_1)} \qquad (d = d_1 t)$$

$$= \prod_{d_1 \mid n} F(d_1)^{\sum_{t \mid (n/d_1)} \mu(n/td_1)}$$

$$= \prod_{\substack{d_1 | n \\ n = d_1}} F(d_1)$$

$$= F(n) \qquad \#$$