初等数论习题课

张神星

摘要. 本文为 2016 年春中国科学院大学课程《初等数论》习题课讲义, 课程所用教材为《华罗庚文集数论卷 II》的《数论导引》.

本文中所用记号:

- $v_p(x)$ 表示非零有理数 x 的素数 p 幂次;
- $p^e \| n$ 表示 $p^e \mid n$ 且 $p^{e+1} \nmid n$;
- μ 表示 Mobiüs 函数;
- $\#$ 表示集合的大小;
- $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p$ 分别表示自然数集, 整数环, 有理数域, 实数域, 复数域, p 元有限域.

第一章　整数之分解

1.1 由于

$$\begin{aligned}
& [\alpha] \leqslant \alpha < [\alpha]+1 \\
\Longrightarrow \quad & n[\alpha] \leqslant n\alpha < n[\alpha]+n \\
\Longrightarrow \quad & n[\alpha] \leqslant [n\alpha] < n[\alpha]+n \\
\Longrightarrow \quad & [\alpha] \leqslant \frac{[n\alpha]}{n} < [\alpha]+1 \\
\Longrightarrow \quad & [\alpha] \leqslant \left[\frac{[n\alpha]}{n}\right] < [\alpha]+1
\end{aligned}$$

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

1.2 设 $k = [n\alpha] - n[\alpha]$, 则

$$\frac{k}{n} \leqslant \alpha - [\alpha] < \frac{k+1}{n}, \quad 0 \leqslant k \leqslant n-1,$$

于是

$$[\alpha] + \frac{k+i}{n} \leqslant \alpha + \frac{i}{n} < [\alpha] + \frac{k+i+1}{n}.$$

因此

$$\left[\alpha + \frac{i}{n}\right] = \begin{cases} [\alpha], & 若\ i < n-k; \\ [\alpha]+1, & 若\ i \geqslant n-k. \end{cases}$$

日期 2016 年 7 月 1 日.

故

$$[\alpha]+\left[\alpha+\frac{1}{n}\right]+\cdots+\left[\alpha+\frac{n-1}{n}\right]=n[\alpha]+k=[n\alpha].$$

1.3 设 $x=\alpha-[\alpha], y=\beta-[\beta]$, 则

$$([2\alpha]+[2\beta])-([\alpha]+[\alpha+\beta]+[\beta])=[2x]+[2y]-[x+y].$$

若 $x>\frac{1}{2}$ 或 $y>\frac{1}{2}$, 则 $[2x]+[2y]\geqslant 1\geqslant[x+y]$; 若 x,y 均 $<\frac{1}{2}$, 则 $x+y<1$, $[2x]+[2y]-[x+y]=0$. 综上所述

$$[2\alpha+2\beta]>[\alpha]+[\alpha+\beta]+[\beta].$$

4 补充 设 $a>1, m, n$ 为正整数, 证明 $(a^m-1, a^n-1)=a^{(m,n)}-1$.

证明. 利用辗转相除法，我们有

$$\begin{aligned}
m&=nq_0+r_0,\quad 0<r_0<n;\\
n&=r_0q_1+r_1,\quad 0<r_1<r_1;\\
&\cdots\\
r_{k-2}&=r_{k-1}q_k+r_k,\quad 0<r_k<r_{k-1};\\
r_{k-1}&=r_kq_{k+1},
\end{aligned}$$

则 $r_k=(m,n)$. 于是

$$\begin{aligned}
a^m-1&=a^{r_0}(a^n-1)(a^{n(q_0-1)}+\cdots+1)+a^{r_0}-1;\\
a^n-1&=a^{r_1}(a^{r_0}-1)(a^{r_0(q_1-1)}+\cdots+1)+a^{r_1}-1;\\
&\cdots\\
a^{r_{k-2}}-1&=a^{r_k}(a^{r_{k-1}}-1)(a^{r_{k-1}(q_k-1)}+\cdots+1)+a^{r_k}-1;\\
a^{r_{k-1}}-1&=(a^{r_k}-1)(a^{r_k(q_{k+1}-1)}+\cdots+1),
\end{aligned}$$

因此 $(a^m-1, a^n-1)=a^{r_k}-1=a^{(m,n)}-1$. □

另证. 我们对 $m+n$ 归纳.

若 $m+n=2$, 显然.

假设命题对于 $m+n\leqslant k-1$ 成立. 对于 $m+n=k$, 不妨设 $m\geqslant n$. 若 $n=0$ 或 $m=n$, 显然成立; 否则 $0<n<m$,

$$a^m-1=a^{m-n}(a^n-1)+a^{m-n}-1,$$

因此 $(a^m-1, a^n-1)=(a^{m-n}-1, a^n-1)$. 由归纳假设, 此为

$$a^{(m-n,n)}-1=a^{(m,n)}-1.$$ □

6.2 以第一个等式为例. 令 $a_k = p_1^{e_{1,k}} \cdots p_s^{e_{s,k}}$, $p_1 < p_2 < \cdots < p_s, e_{i,k} \geqslant 0$. 则

$$v_{p_i}(a_1 \cdots a_n) = \sum_{k=1}^{n} e_{i,k}$$

$$v_{p_i}(a_1 \cdots a_{j-1} a_{j+1} \cdots a_n) = \sum_{k=1}^{n} e_{i,k} - e_{i,j}$$

$$v_{p_i}(\text{右边}) = \sum_{k=1}^{n} e_{i,k} - \max_j \{ \sum_{k=1}^{n} e_{i,k} - e_{i,j} \} = \min_j \{ e_{i,j} \} = v_{p_i}(\text{左边}).$$

因此两边相等.

8.2 由于

$$n = bcx + cay + abz = bc(x + at + as) + ca(y - bs) + ab(z - ct),$$

我们不妨设 $0 \leqslant y < b, 0 \leqslant z < c$, 于是

$$x = \frac{n - cay - abz}{bc} \geqslant \frac{n - ca(b-1) - ab(c-1)}{bc} = \frac{n - 2abc + ac + ab}{bc}.$$

若 $n > 2abc - ac - ab - bc$, 则上式大于 -1, 因此必然 $\geqslant 0$. 也就是说, 任意大于 $2abc - ab - bc - ca$ 的整数 n 均可由此表出.

若 $n = 2abc - ab - bc - ca = bcx + cay + abz$, 则

$$bc(x+1) + ca(y+1) + ab(z+1) = 2abc.$$

若 $x, y, z \geqslant 0$, 则 $x+1, y+1, z+1 \geqslant 1$ 且 $a \mid x+1, b \mid y+1, c \mid z+1$, 因此

$$x + 1 \geqslant a, y + 1 \geqslant b, z + 1 \geqslant c,$$

$$bc(x+1) + ca(y+1) + ab(z+1) \geqslant 3abc,$$

这不可能!

8.3 设该方程的解数为 a_n, 则我们有

$$\begin{aligned} f(T) =& \frac{1}{(1-T)(1-T^2)(1-T^3)} \\ =& (1 + T + T^2 + \cdots)(1 + T^2 + T^4 + \cdots)(1 + T^3 + T^6 + \cdots) \\ =& \sum_{x,y,z \geqslant 0} T^{x+2y+3z} = \sum_n a_n T^n. \end{aligned}$$

通过待定系数, 我们有

$$\begin{aligned}
&f(T)\\
=&\frac{1}{6(1-T)^3}+\frac{1}{4(1-T)^2}+\frac{17}{72(1-T)}+\frac{1}{8(1+T)}+\frac{1}{9}(\frac{1}{1-\omega T}\\
&\quad+\frac{1}{1-\bar{\omega}T})\\
=&\sum_n(\frac{1}{6}\frac{(n+1)(n+2)}{2}+\frac{1}{4}(n+1)+\frac{17}{72}+\frac{(-1)^n}{8}+\frac{2}{9}\cos\frac{2n\pi}{3})T^n\\
=&\sum_n(\frac{(n+3)^2}{12}-\frac{7}{72}+\frac{(-1)^n}{8}+\frac{2}{9}\cos\frac{2n\pi}{3})T^n.
\end{aligned}$$

9.2 设 $n=\prod\limits_{i=1}^{s}p_i^{e_i}$, 则

$$\begin{aligned}
\prod_{d\mid n}d&=\prod_{x_1=0}^{e_1}\prod_{x_2=0}^{e_2}\cdots\prod_{x_s=0}^{e_s}\prod_{i=1}^{s}p_i^{x_i}\\
&=\prod_{i=1}^{s}(\prod_{x_i=0}^{e_i}p_i^{x_i})^{\tau(n)/(e_i+1)}\\
&=\prod_{i=1}^{s}p_i^{\tau(n)e_i/2}=n^2,
\end{aligned}$$

其中 $\tau(n)=\prod\limits_{i=1}^{s}(e_i+1)$ 为 n 的正因子个数. 因此 $\tau(n)=4$,

$$s=1,e_1=3\text{ 或 }s=2,e_1=e_2=1,$$

n 为一素数之立方或两不同素数之积.

另证. 由于

$$\prod_{d\mid n}d=\prod_{d\mid n}\frac{n}{d}=\frac{n^{\tau(n)}}{\prod_{d\mid n}d},$$

因此 $\prod\limits_{d\mid n}d=n^{\tau(n)/2}$, $\tau(n)=4$. 其余与上文相同. □

9 补充 记 n 的因子个数为 $\tau(n)$.

(1) 证明 $\tau(n)\leqslant 2\sqrt{n}$.

(2) 证明 $\tau(n)\leqslant\sqrt{3n}$.

(3) 证明 $\tau(n)\leqslant 8\sqrt[3]{\frac{3n}{35}}$.

证明. (1) 由于 $d\mid n$ 等价于 $\frac{n}{d}\mid n$, 因此

$$\tau(n)\leqslant 2\lceil\sqrt{n}\rceil+1\leqslant 2\sqrt{n},$$

其中 $\lceil x\rceil$ 为不小于 x 的最小的整数.

(2) 对任意 $\lambda > 0$ 和素数 p, 我们考虑 $f_p(v) = \frac{p^{\lambda v}}{v+1}$ 的最小值, 其中 v 是自然数. 由于

$$f_p(v) \leqslant f_p(v-1) \iff \frac{p^{\lambda v}}{v+1} \leqslant \frac{p^{\lambda v-1}}{v} \iff v \leqslant \frac{1}{\sqrt{p}-1},$$

$$f_p(v) \leqslant f_p(v+1) \iff v+1 \geqslant \frac{1}{\sqrt{p}-1},$$

因此

$$\min_{v\in\mathbb{N}} f_p(v) = f_p([\frac{1}{\sqrt{p}-1}]).$$

若 $\lambda = \frac{1}{2}$, 则

$$\frac{\sqrt{n}}{\tau(n)} = \prod_p \frac{\sqrt{p}^{e_p}}{e_p+1} \geqslant f_2(2)f_3(1) = \frac{2}{3} \times \frac{\sqrt{3}}{2} = \frac{1}{\sqrt{3}}.$$

若 $\lambda = \frac{1}{3}$, 则

$$\frac{\sqrt[3]{n}}{\tau(n)} \geqslant f_2(3)f_3(2)f_5(1)f_7(1) = \frac{1}{2} \times \frac{\sqrt[3]{3^2}}{3} \times \frac{\sqrt[3]{5}}{2} \times \frac{\sqrt[3]{5}}{2} = \frac{1}{8}\sqrt[3]{\frac{35}{3}}.$$

□

10 补充 证明若正整数 $m > n$, 则 $F_n \mid (F_m - 2)$ 且 $(F_m, F_n) = 1$. 由此证明素数有无穷多个.

证明. 由于

$$F_m - 2 = 2^{2^m} - 1 = (2^{2^n} - 1)\prod_{k=n}^{m-1} \frac{2^{2^{k+1}} - 1}{2^{2^k} - 1} = (F_n - 2)\prod_{k=n}^{m-1} F_k,$$

因此 $F_n \mid (F_m - 2)$ 且 $(F_m, F_n) = (2, F_n) = 1$. 由此可知 F_n 两两互素, 它们含有不同的素因子, 因此素数有无穷多个. □

11.2 $\binom{1000}{500}$ 的 5 的幂次为

$$\begin{aligned} v_5(\binom{1000}{500}) &= \sum_{k\geqslant 1}(\left[\frac{1000}{5^k}\right] - 2\left[\frac{500}{5^k}\right]) \\ &=(200 - 2\times 100) + (40 - 2\times 20) + (8 - 2\times 4) + 1 = 1. \end{aligned}$$

11 补充 1 设 m, n 为正整数, 证明 $\dfrac{(2m+2n)!}{(m+n)!m!n!}$ 为整数.

证明. 由习题 1.3 可知

$$[\frac{2m+2n}{p^t}] \geqslant [\frac{m+n}{p^t}] + [\frac{m}{p^t}] + [\frac{n}{p^t}],$$

因此

$$v_p\left(\frac{(2m+2n)!}{(m+n)!m!n!}\right) \geqslant 0.$$

由于 p 是任意的, 因此原命题成立. □

11 补充 2 设 a,b 为不同的正整数, n 为正整数. 如果 $n \mid a^n-b^n$, 则 $n \mid \dfrac{a^n-b^n}{a-b}$.

证明. 设 $p^e \| n$, 即 n 的 p 的幂次为 e, 则 $a^{p^e}-b^{p^e} \mid a^n-b^n$. 设 $p^f \| i \geqslant 1$, 则 $p^{e-f} \| \binom{p^e}{i}$. 若 $p \nmid b$, 则

$$a^{p^e}-b^{p^e}=\sum_{i=1}^{p^e}\binom{p^e}{i}(a-b)^i b^{p^e-i}$$

的 p 之方次数 $\geqslant e-f+i \geqslant e+1$, 即 $p^e \mid \frac{a^n-b^n}{a-b}$.

若 $p \mid b$, 设 $p^f \| a-b$, 则

$$a^{p^e}-b^{p^e}=\sum_{i=1}^{p^e}\binom{p^e}{i}(a-b)^i b^{p^e-i}$$

的 p 之方次数 $\geqslant fi+p^e-i \geqslant fi+e+1-i \geqslant e+f$, 即 $p^e \mid \frac{a^n-b^n}{a-b}$. □

12.1 凡 k 次 n 元之整值多项式必可表为

$$\sum_{\lambda_1+\cdots+\lambda_n \leqslant k} \alpha_{\lambda_1,\ldots,\lambda_n}\binom{x_1}{\lambda_1}\cdots\binom{x_n}{\lambda_n},$$

式中 $\alpha_{\lambda_1,\ldots,\lambda_n}$ 皆为整数, 且对任何整数 $\alpha_{\lambda_1,\ldots,\lambda_n}$, 此皆整值多项式.

证明. 1) 如此之多项式显然是整值多项式.

2) $n=1$ 时由定理 2 知成立. $n \geqslant 2$ 时, 若命题对 $n-1$ 已成立, 由于任一 k 次 n 元整值多项式 $f(x_1,\ldots,x_n)$ 可写成

$$f(x_1,\ldots,x_n)=\sum_{i=0}^{k}\alpha_i(x_2,\ldots,x_n)\binom{x_1}{i},$$

由归纳假设可得. □

12.3 设 k 为正整数, 如果 $k=m+\frac{1}{2}(m+n-1)(m+n-2)$, 则

$$\frac{1}{2}(m+n-1)(m+n-2) \leqslant k-1 < m+n-1+\frac{1}{2}(m+n-1)(m+n-2),$$

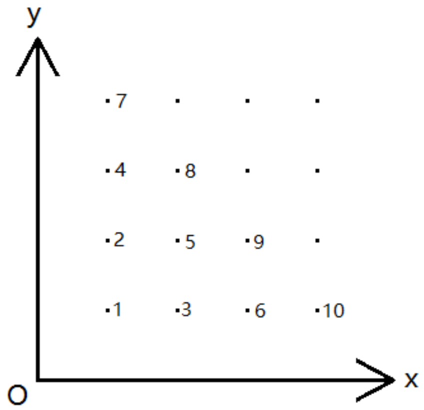
整理可得

$$m+n=e=\left[\sqrt{2k-\frac{7}{4}}+\frac{1}{2}\right]+1,$$

$$1 \leqslant m = k-\frac{1}{2}e(e-1) < e,$$

即 k 可以唯一地写成题述形式.

另证: 将正整数按下图顺序排在第一象限, 则直线 $x+y=e$ 上最大的数为 $e(e-1)/2$, 坐标 (m,n) 处的数为 $\frac{1}{2}(m+n-1)(m+n-2)+m$, 它们无重复无遗漏地取遍所有正整数.



12.4 设 k 次多项式 $f(x)$ 在 $a, a+1, \ldots, a+k$ 处取整数值, 令 $g(x) = f(x+a)$, 则 $g(0), g(1), \ldots, g(k) \in \mathbb{Z}$. 设 $g(x) = \sum_{i=0}^{k} \alpha_i \binom{x}{i}$, 则

$$\alpha_k = \Delta^k g \mid_{x=0} = \sum_{i=0}^{k} (-1)^{k-i} \binom{k}{i} g(i) \in \mathbb{Z},$$

因此 $g(x)$ 是整值多项式, $f(x)$ 也是.

13 设 $f(x) = x^6 + x^3 + 1$, 则

$$f(x+1) = x^6 + 6x^5 + 15x^4 + 21x^3 + 18x^2 + 9x + 3.$$

令 $p = 3$, 由 Eisenstein 判别法可知 f 不可约.

13 补充 1 设 $a_1, \ldots, a_n$ 为两两不同的整数, 证明 $(x-a_1)\cdots(x-a_n)-1$ 不可约.

证明. 假设 $f(x) = (x-a_1)\cdots(x-a_n)-1$ 可约, 由于 f 首一, 存在首一的非常数整系数多项式 $g(x), h(x)$, $f(x) = g(x)h(x)$. 于是 $g(a_i) = \pm 1$. 不妨设 $g(a_1) = \cdots = g(a_t) = 1, g(a_{t+1}) = \cdots = g(a_n) = -1$, 则 $\deg g \geq \max\{t, n-t\}$, 同理 $\deg h \geq \max\{t, n-t\}$. 因此 $t = n-t = \deg g = \deg h$,

$$g(x) = (x-a_1)\cdots(x-a_t)+1, \ \ h(x) = (x-a_1)\cdots(x-a_t)-1,$$

$$f(x) = g(x)h(x) = (x-a_1)^2\cdots(x-a_t)^2 - 1,$$

矛盾! □

13 补充 2 设 $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x], a_0 \neq 0$. 证明: 如果 $|a_{n-1}| > 1 + |a_0| + \cdots + |a_{n-2}|$, 则 $f(x)$ 不可约.

证明. f 的常数项模长大于等于 1, 因此存在根 x_0, $|x_0| \geq 1$. 设

$$g(x) = \frac{f(x)}{x-x_0} = x^{n-1} + \sum_{i=0}^{n-2} b_i x^i,$$

则

$$\begin{aligned} a_0 &= -x_0 b_0, \\ a_i &= -x_0 b_i + b_{i-1}, \quad 1 \leqslant i \leqslant n-2, \\ a_{n-1} &= -x_0 + b_{n-2}, \end{aligned}$$

于是

$$\begin{aligned} |b_{n-2}| + |x_0| \geq |b_{n-2} - x_0| &= |a_{n-1}| \\ &> 1 + \sum_{i=0}^{n-2} |a_i| \\ &= 1 + \sum_{i=0}^{n-2} |x_0 b_i - b_{i-1}| \\ &\geq 1 + \sum_{i=0}^{n-2} (|x_0 b_i| - |b_{i-1}|) \\ &= (|x_0| - 1) \sum_{i=0}^{n-2} |b_i| + |b_{n-2}| + 1 \end{aligned}$$

$$(|x_0| - 1)(\sum_{i=0}^{n-2} |b_i| - 1) < 0,$$

因此 $|x_0| > 1, \sum_{i=0}^{n-2} |b_i| < 1$.

设 $g(x) = (x - y_0)(x^{n-2} + \sum_{i=0}^{n-3} c_i x^i)$, 则类似地, 我们有

$$1 > \sum_{i=0}^{n-2} |b_i| \geq (|y_0| - 1) \sum_{i=0}^{n-3} |c_i| + |y_0|,$$

$$(|y_0| - 1)(\sum_{i=0}^{n-3} |c_i| + 1) < 0,$$

$|y_0| < 1$. 因此 f 只有一个根模长大于 1, 其余模长均小于 1. 如果 $f = gh$ 可约, 则 g, h 的常数项均非零, 均存在模长大于等于 1 的根, 矛盾! 因此 f 不可约.

实际上, 如果我们利用复变函数中儒歇定理, 可以知道在 S^1 上 $|f - a_{n-1}x^{n-1}| < |a_{n-1}x^{n-1}|$, 从而 f 和 $a_{n-1}x^{n-1}$ 在 S^1 内部有相同多的根, 即 $n-1$ 个. □

第二章 同余式

2 补充 (1) 设 n 是整数, 证明 $n^2 \equiv 0, 1 \bmod 4, n^3 \equiv 0, 1 \bmod 9, n^4 \equiv 0, 1 \bmod 16$.

(2) 设 a 是奇数, n 是正整数, 证明 $a^{2^n} \equiv 1 \bmod 2^{n+2}$.

证明. (1) 若 $n=2k$, 则 $n^2=4k^2\equiv 0 \bmod 4$; 若 $n=2k+1$, 则 $n^2=4k^2+4k+1\equiv 1 \bmod 4$.

若 $n=3k$, 则 $n^3=27k^3\equiv 0 \bmod 9$; 若 $n=3k\pm 1$, 则 $n^3=27k^3\pm 27k^2+9k\pm 1\equiv 1 \bmod 9$.

若 $n=2k$, 则 $n^4=16k^4\equiv 0 \bmod 16$; 若 $n=4k\pm 1$, 则 $n^4=256k^4\pm 256k^3+96k^2\pm 16k+1\equiv 1 \bmod 16$.

(2) 由于

$$a^{2^n}-1=(a+1)(a-1)\prod_{i=2}^{n-1}(a^{2^i}+1),$$

而 $a+1$ 和 $a-1$ 有一个为 4 的倍数, 因此 $2^{n+2}\mid a^{2^n}-1$. □

3 补充 1 设 m,n 是正整数, $(m,n)=1$. 证明:

$$m^{\varphi(n)}+n^{\varphi(m)}\equiv 1 \bmod mn.$$

证明. 由于 $m^{\varphi(n)}\equiv 1 \bmod n$, 因此 $m^{\varphi(n)}+n^{\varphi(m)}\equiv 1 \bmod m$. 同理 $m^{\varphi(n)}+n^{\varphi(m)}\equiv 1 \bmod n$, 因此原命题成立. □

3 补充 2 设 p,q 为不同的奇素数, a 与 p,q 互素, 证明

$$a^{\varphi(pq)/2}\equiv 1 \bmod pq.$$

证明. 由于 p,q 为奇数, $a^{p-1}\equiv 1 \bmod p$, 因此 $a^{(p-1)(q-1)/2}\equiv 1 \bmod p$. 同理对 q 成立. □

5.1 设 $m=\prod p^e, d=\prod p^f, f\leqslant e$, 则

$$\varphi(d)=\prod\varphi(p^f),$$

$$\sum_{d\mid m}\varphi(d)=\prod\sum_{0\leqslant f\leqslant e}\varphi(p^f)=\prod(1+\sum_{1\leqslant f\leqslant e}(p^f-p^{f-1}))=\prod p^e=m.$$

5 补充 1 令

$$\mu(n)=\begin{cases}1, & n=1;\\ (-1)^k, & n=p_1\cdots p_k, p_i \text{ 两两不同};\\ 0, & n \text{ 有平方因子},\end{cases}$$

则

$$\varphi(n)=\sum_{d\mid n}d\mu(\frac{n}{d}), n=\sum_{d\mid n}\varphi(d).$$

一般地, 若

$$f(n)=\sum_{d\mid n}g(d),$$

则

$$g(n)=\sum_{d\mid n}f(d)\mu(\frac{n}{d}).$$

5.2 由

$$\frac{\varphi(mn)}{\varphi(m)\varphi(n)}=\frac{mn\prod\limits_{p\mid mn}(1-\frac{1}{p})}{m\prod\limits_{p\mid m}(1-\frac{1}{p})\times n\prod\limits_{p\mid n}(1-\frac{1}{p})}$$
$$=\frac{1}{\prod\limits_{p\mid (m,n)}(1-\frac{1}{p})}=\frac{1}{\prod\limits_{p\mid P}(1-\frac{1}{p})}=\frac{P}{\varphi(P)}$$

可得.

5 补充 2 (1) 当 $n\geqslant 3$ 时, $\varphi(n)$ 是偶数.

(2) 当 $n\geqslant 2$ 时, 不超过 n 且与 n 互素的正整数之和是 $\frac{1}{2}n\varphi(n)$.

证明. (1) 由于 $(a,n)=(n-a,n)=1$ 且若 n 为偶数时, $(\dfrac{n}{2},n)\neq 1$, 因此

$$\varphi(n)=2\#\{1\leqslant a<\frac{n}{2}\mid (a,n)=1\}$$

为偶数.

或者: 若存在奇素数 $p\mid n$, 则 $(p-1)\mid\varphi(n)$ 为偶数. 若不然, 则 $n=2^k$, $k\geq 2$, 因此 $\varphi(n)=2^{k-1}$ 为偶数.

(2) 由于 $(a,n)=(n-a,n)=1$, 因此

$$\sum_{1\leqslant a\leqslant n,(a,n)=1}a=\sum_{1\leqslant a\leqslant n,(a,n)=1}(n-a)=\frac{1}{2}\sum_{1\leqslant a\leqslant n,(a,n)=1}n=\frac{1}{2}n\varphi(n).\quad\square$$

5 补充 3 (1) 设 $f(n),g(n)$ 是积性函数, 证明

$$(f*g)(n)=\prod_{d\mid n}f(d)g(n/d)$$

也是积性函数.

(2) 证明所有不恒为 0 的积性函数关于 $*$ 构成交换群, 且 $\mathbb{1}^{-1}=\mu$, 这里 $\mathbb{1}$ 表示常值函数 1.

证明. (1) 若 $d\mid m,e\mid n$, $(m,n)=1$, 则 $(d,e)=1,(m/d,n/e)=1$, 因此

$$(f*g)(mn)=\prod_{d\mid mn}f(d)g(mn/d)=\prod_{d\mid m,e\mid n}f(de)g(mn/de)$$
$$=\prod_{d\mid m,e\mid n}f(d)f(e)g(m/d)g(n/e)=\prod_{d\mid m}f(d)g(m/d)\times\prod_{e\mid n}f(e)g(n/e)$$
$$=(f*g)(m)\times(f*g)(n).$$

(2) 设 $e(1)=1, e(n)=0, n\geqslant 2$, 则易见 $f*g=g*f, f*e=e*f$.

$$((f*g)*h)(n)=\prod_{d|n}(f*g)(d)h(n/d)$$
$$=\prod_{e|d|n}f(e)g(d/e)h(n/d)=\prod_{e|n,d'|n/e}f(e)g(d')h(n/d'e)$$
$$=\prod_{e|n}f(e)(g*h)(n/e)=(f*(g*h))(n).$$

由 $f(1)f(n)=f(n)$ 知若 f 不恒为 0, 则 $f(1)\neq 0$, 定义

$$g(1)=f(1)^{-1}, g(n)=-f(1)^{-1}\sum_{d|n,d\neq n}f(n/d)g(d),$$

则 g 为积性函数且 $f*g=e$.
易知 $(\mu*\mathbb{1})(n)=\prod_{d|n}\mu(d)=e(n)$. □

9 补充 设 G 是有限 Abel 群, 则

$$\prod_{g\in G}g=\prod_{a\in G,a^2=1}a.$$

由此, 对正整数 m, 计算

$$\prod_{1\leqslant a\leqslant m,(a,m)=1}a \bmod m.$$

证明. 由于 $g^2\neq 1$ 当且仅当 $g\neq g^{-1}$, 这样的 g 可以两两配对成互为逆的对, 于是命题可得.
令 $G=(\mathbb{Z}/m\mathbb{Z})^{\times}$, 设 $x^2\equiv 1 \bmod m$.
若 $m=2^k$, 则 $x=\pm 1, \pm 1+2^{k-1}$.
若 $m=p^k$, 则 $x=\pm 1$.
因此当 $4\mid m$ 且 m 有奇素因子, 或 m 有至少两个不同的奇素因子时, 上式为 1.
当 $m=p^k, 2p^k$ 且 $k\geqslant 1$, p 为素数时, 上式为 -1. □

第三章 二次剩余

2 设 $p=4n+3$, $q=8n+7$ 为素数, 则

$$2^p=2^{\frac{q-1}{2}}\equiv\left(\frac{2}{q}\right)=1 \mod q,$$

因此 $q\mid 2^p-1$. 令 p 为相应的素数即可得到题目中的关于 Mersenne 素数的结论.

6 补充 1 设 p 是素数, $p\equiv 1 \pmod 4$. 证明

(1) $\sum\limits_{r=1,\left(\frac{r}{p}\right)=1}^{p-1} r=\frac{p(p-1)}{4}$;

(2) $\sum\limits_{r=1}^{p-1} r\left(\frac{r}{p}\right)=0$;

(3) $\sum\limits_{r=1}^{\frac{p-1}{2}}\left[\frac{r^2}{p}\right]=\frac{(p-1)(p-5)}{24}$.

证明. (1) 由于 $\left(\frac{p-r}{p}\right)=\left(\frac{-r}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{r}{p}\right)=\left(\frac{r}{p}\right)$, 因此

$$\sum_{r=1,\left(\frac{r}{p}\right)=1}^{p-1} r=\frac{1}{2}\sum_{r=1,\left(\frac{r}{p}\right)=1}^{p-1} p=\frac{p(p-1)}{4}.$$

(2) 我们有

$$\sum_{r=1}^{p-1} r\left(\frac{r}{p}\right)=2\sum_{r=1,\left(\frac{r}{p}\right)=1}^{p-1} r-\sum_{r=1}^{p-1} r=0.$$

(3) 由于此时 r^2 取遍 $\bmod p$ 的二次非剩余, 因此

$$\begin{aligned}\sum_{r=1}^{\frac{p-1}{2}}\left[\frac{r^2}{p}\right]&=\sum_{r=1}^{\frac{p-1}{2}}\frac{r^2}{p}-\sum_{r=1,\left(\frac{r}{p}\right)=1}^{p-1}\frac{r}{p}\\&=\frac{1}{6}\times\frac{p-1}{2}\times\frac{p+1}{2}-\frac{p-1}{4}\\&=\frac{(p-1)(p-5)}{24}.\end{aligned}$$

□

6 补充 2 设 $p>3$ 是素数, $p\equiv 3 \pmod 4$. 证明

(1) $\sum\limits_{r=1,\left(\frac{r}{p}\right)=1}^{p-1} r\equiv 0 \pmod p$;

(2) $\sum\limits_{a=1}^{p-1} a\left(\frac{a}{p}\right)\equiv 0 \pmod p$.

证明. (1) 由于 $1^2,2^2,\ldots,(\dfrac{p-1}{2})^2$ 取遍 $\bmod p$ 的所有二次剩余, 因此

$$\sum_{r=1,\left(\frac{r}{p}\right)=1}^{p-1} r\equiv\sum_{s=1}^{(p-1)/2} s^2=\frac{p(p^2-1)}{24}\equiv 0 \pmod p.$$

(2) 我们有

$$\sum_{r=1}^{p-1} r\left(\frac{r}{p}\right)=2\sum_{r=1,\left(\frac{r}{p}\right)=1}^{p-1} r-\sum_{r=1}^{p-1} r\equiv\frac{(p-1)p}{2}\equiv 0 \pmod p.$$

□

6 补充 3 证明方程 $x^2-y^2\equiv n \bmod p$ 在 mod$p$ 意义下的解的个数为 $p-1$, 若 $p\nmid n$; 为 $2p-1$, 若 $p\mid n$.

证明. 若 $p\mid n$, 则所有解为

$$(s,\pm s),(-s,\pm s),(0,0),\quad s=1,2,\ldots,p-1,$$

共 $2p-1$ 个解. 若 $p\nmid n$, 令 $s=x+y$, 则 $x-y\equiv ns^{-1}\bmod p$, 所有解为

$$(\frac{s+ns^{-1}}{2},\frac{s-ns^{-1}}{2}),\quad s=1,2,\ldots,p-1,$$

共 $p-1$ 个解. □

6 补充 4 设 p 是奇素数, $f(x)=ax^2+bx+c$ 且 $p\nmid a$. 记

$$D=b^2-4ac.$$

证明

$$\sum_{x=0}^{p-1}\left(\frac{f(x)}{p}\right)=\begin{cases}-\left(\frac{a}{p}\right), & \text{如果 } p\nmid D,\\ (p-1)\left(\frac{a}{p}\right), & \text{如果 } p\mid D.\end{cases}$$

这里 $\left(\frac{0}{p}\right)=0$.

证明. 易知方程 $x^2\equiv -D\bmod p$ 的解的个数为 $1+\left(\frac{-D}{p}\right)$, 因此由上一题结论知

$$\sum_{y=0}^{p-1}(1+\left(\frac{y^2-D}{p}\right))=\begin{cases}p-1, & \text{如果 } p\nmid D,\\ 2p-1, & \text{如果 } p\mid D.\end{cases}$$

由于 $4af(x)=(2ax+b)^2-D$, 因此

$$\begin{aligned}\sum_{x=0}^{p-1}\left(\frac{f(x)}{p}\right)&=\left(\frac{a}{p}\right)\sum_{x=0}^{p-1}\left(\frac{x^2-D}{p}\right)\\&=\begin{cases}-\left(\frac{a}{p}\right), & \text{如果 } p\nmid D,\\ (p-1)\left(\frac{a}{p}\right), & \text{如果 } p\mid D.\end{cases}\end{aligned}$$

□

6 补充 5 方程 $x^2-ay^2\equiv n\bmod p$ 在 mod$p$ 意义下的解的个数为多少?

解. 方程 $x^2-ay^2\equiv n\bmod p$ 的解的个数为

$$\begin{aligned}\sum_{y=0}^{p-1}(1+\left(\frac{ay^2+n}{p}\right))&=p+\left(\frac{a}{p}\right)\sum_{y=0}^{p-1}\left(\frac{y^2+na^{-1}}{p}\right)\\&=\begin{cases}p-\left(\frac{a}{p}\right), & \text{如果 } p\nmid D,\\ p+(p-1)\left(\frac{a}{p}\right), & \text{如果 } p\mid D.\end{cases}\end{aligned}$$

□

6 补充 6 试问方程

$$a_1x_1^2+\cdots+a_kx_k^2=c$$

在 $\mathbb{F}_p$ 上有多少个解? 这里 $a_i\neq 0$.

6 补充 7 若非零整数 a 对所有素数都不是二次非剩余, 则 a 是平方数.

证明. 不妨设 a 无平方因子. 由于

$$\left(\frac{-1}{3}\right)=-1,\quad \left(\frac{\pm 2}{5}\right)=-1,$$

故 $a\neq -1,\pm 2$. 若 a 存在奇素因子 p. 设 $a=\pm 2^{\varepsilon}pn$, 由中国剩余定理知存在 $m\equiv 1 \bmod 8n$ 且 m 是模 p 的二次剩余. 由狄利克雷定理知存在素数 $q\equiv m \bmod 8pn$, 于是

$$\left(\frac{a}{q}\right)=\left(\frac{pn}{q}\right)=\left(\frac{q}{pn}\right)=\left(\frac{m}{pn}\right)=\left(\frac{m}{p}\right)=-1,$$

矛盾! 因此 $a=1$. □

8 补充 1 设 p 是奇素数. 证明: 模 p 的任意两个原根之积不是模 p 的原根.

证明. 设 a,b 是模 p 的原根, 则 $b=a^e$ 且 $(e,p-1)=1$. 因此 e 为奇数, $e+1$ 为偶数,

$$(ab)^{\frac{p-1}{2}}=(a^{\frac{e+1}{2}})^{p-1}\equiv 1 \bmod p,$$

故 ab 不是原根. □

8 补充 2 设 p 与 $q=2p+1$ 都是素数. 证明

(1) 当 $p\equiv 1 \pmod 4$ 时, 2 是模 q 的原根;

(2) 当 $p\equiv 3 \pmod 4$ 时, -2 是模 p 的原根.

证明. (1) 由于 $q\equiv 3 \bmod 8$,

$$2^2=4\not\equiv 1,\quad 2^p=2^{\frac{q-1}{2}}\equiv\left(\frac{2}{q}\right)=-1 \bmod q,$$

而 2 的阶整除 $\varphi(q)=2p$, 因此 2 的阶为 $2p=q-1$, 即 2 是模 q 的原根.

(2) 由于 $q\equiv 7 \bmod 8$,

$$(-2)^2=4\not\equiv 1,\quad (-2)^p=(-2)^{\frac{q-1}{2}}\equiv\left(\frac{-2}{q}\right)=-1 \bmod q,$$

而 -2 的阶整除 $\varphi(q)=2p$, 因此 -2 的阶为 $2p=q-1$, 即 -2 是模 q 的原根. □

8 补充 3 设 n, a 都是正整数且 $a > 1$. 证明 $n \mid \varphi(a^n - 1)$.

证明. 设 d 为 a 模 $a^n - 1$ 的阶, 则由

$$a^n \equiv 1 \mod (a^n - 1)$$

可知 $d \leqslant n$. 另一方面, 若 $d < n$, 则 $a^d - 1 < a^n - 1$, $a^d \not\equiv 1 \mod (a^n - 1)$, 因此 $d \geqslant n$. 故 $d = n$. 再由欧拉定理知

$$n = d \mid \varphi(a^n - 1).$$

□

9 由题设知 n 是奇数. 令 d 为 2 模 n 的阶, 则 $d \nmid k, d \mid n - 1 = kp^2$, 因此 $p \mid d$. 而 $d \mid \varphi(n)$, 因此 $p \mid \varphi(n)$, 于是由欧拉函数的公式可知, 存在素数 $q \mid n$ 且 $q \equiv 1 \mod p$.

若 n 不是素数, 则存在正整数 u, v 使得

$$n = kp^2 + 1 = (up + 1)(vp + 1) = uvp^2 + (u + v)p + 1,$$

于是 $p \mid u + v$, $u + v \geqslant p$. 因此 $uv = (u - 1)(v - 1) + u + v - 1 \geqslant p - 1$,

$$k = uv + (u + v)/p \geqslant p - 1 + 1 = p,$$

矛盾! 因此 n 是素数.

第四章　多项式之性质

4.1 $R = \mathbb{Z}[x_1, \ldots, x_n]$ 的理想为均为有限生成的.

证明. 假设命题对于 $n < k$ 成立. 对于 $n = k$, 我们令 deg 表示 R 中多项式关于 x_k 的次数. 设 $I \subseteq R$ 是非零理想. 记 I 中多项式关于 x_k 的首项系数形成的集合为 J, 则 J 是 $\mathbb{Z}[x_1, \ldots, x_{k-1}]$ 的理想. 由归纳假设, J 是有限生成的, 不妨设由 $a_1, \ldots, a_m$ 生成. 设对应 I 中的多项式为

$$f_i = a_i x_k^{d_i} + \cdots.$$

不妨设 $d = d_1 \geqslant d_2 \geqslant \cdots \geqslant d_m$. 我们断言任一 $f \in I$ 可表为

$$f = \sum_{i=1}^{m} q_i f_i + r,$$

其中 $\deg r < d$. 若 $\deg f < d$, 则已经成立. 若不然, f 关于 x_k 的首项系数可表为

$$\sum_{i=1}^{m} c_i a_i, \quad c_i \in \mathbb{Z}[x_1, \ldots, x_{k-1}],$$

令

$$r := f - \sum_{i=1}^{m} x_k^{\deg f - d_i} c_i f_i,$$

则 $\deg r < \deg f$. 依此法进行下去, 即可得到该结论.

记 I 中次数小于 d 的元素的首项系数行成的集合为 J', 则 J' 也是有限生成的理想, 记其生成元对应的 I 中多项式为 $g_1, \ldots$, 其 x_k 最高次数为 $d' < d$. 则类似地, I 中任一次数小于 d 的多项式均可表为

$$r' + q_1' g_1 + \cdots$$

且 $\deg r' < d'$. 按此法进行下去, $d, d', \ldots$ 会越来越小, 直至为 0. 因此 I 被这些 $f_i, g_j, \ldots$ 生成, 故为有限生成.

又因为 $n = 0$ 命题显然成立, 因此由归纳法知原命题成立. $\square$

4.2 设 R 为所有 $\mathbb{Q}[x]$ 中整值多项式形成的环. 令 I 为所有 $\binom{x}{k}, k \geqslant 1$ 形成的理想. 如果 I 是有限生成的, 不妨设 I 由

$$f_1, \ldots, f_m$$

生成, 且它们的次数为 $d = d_1 \geqslant d_2 \geqslant \cdots d_m$. 则 I 可由

$$\binom{x}{1}, \binom{x}{2}, \ldots, \binom{x}{d}$$

生成. 对于素数 $p > d$,

$$\binom{x}{p} = \sum_{i=1}^{d} \binom{x}{i} g_i(x), \quad g_i \in R.$$

令 $x = p$, 则

$$1 = \sum_{i=1}^{d} \binom{p}{i} g_i(p),$$

由于 $1 \leqslant i \leqslant d < p$, 因此右式是 p 的倍数, 这不可能! 因此 I 不是有限生成的.

4 补充 1 对于 $n \in \mathbb{Z}$, 证明 $x^n + x^{-n}$ 是 $x + x^{-1}$ 的整系数多项式.

证明. 我们只需对 $n \in \mathbb{N}$ 证明. $n = 0, 1$ 显然. 若命题对于 $n \leqslant k$ 均成立, 则

$$x^{k+1} + x^{-k-1} = (x + x^{-1})(x^k + x^{-k}) - (x^{k-1} + x^{-k+1})$$

也是 $x + x^{-1}$ 的整系数多项式. 由归纳法知对任意 $n \in \mathbb{N}$, $x^n + x^{-n}$ 是 $x + x^{-1}$ 的整系数多项式. $\square$

4 补充 2 设 x_1, x_2, x_3 是整系数三次方程 $x^3 + ax^2 + bx + c = 0$ 的根. 记 $a_n = x_1^n + x_2^n + x_3^n$. 证明对 $n \in \mathbb{N}$, a_n 是整数.

证明. $n = 0, 1, 2$ 时, $a_0 = 3, a_1 = -a, a_2 = a^2 - 2b$ 是整数. 若命题对 $n \leqslant k \leqslant 2$ 成立, 则

$$x_i^{k+1} + ax_i^k + bx_i^{k-1} + cx_i^{k-2} = 0, \quad k \geqslant 2,$$

于是 $a_{k+1} = -aa_k - ba_{k-1} - ca_{k-2}$ 是整数. 由归纳法知对任意 $n \in \mathbb{N}$, a_n 是整数. $\square$

4 补充 3 设 $f(x) \in \mathbb{Q}[x]$ 是一个 n 次多项式, 满足

$$f(k) = 2^k \ (k = 1, 2, \cdots, n+1).$$

求 $f(n+2)$.

解. 由 Lagrange 插值公式知

$$f(x) = \sum_{k=1}^{n+1} f(k) \prod_{i=1, i\neq k}^{n+1} \frac{x-i}{k-i},$$

于是

$$\begin{aligned} f(n+2) &= \sum_{k=1}^{n+1} 2^k \prod_{i=1, i\neq k}^{n+1} \frac{n+2-i}{k-i} \\ &= \sum_{k=1}^{n+1} 2^k (-1)^{n+1-k} \frac{(n+1)!}{(k-1)!(n+2-k)!} \\ &= \sum_{k=0}^{n} 2^{k+1} (-1)^{n-k} \binom{n+1}{k} \\ &= 2^{n+2} - 2 \sum_{k=0}^{n+1} 2^k (-1)^{n+1-k} \binom{n+1}{k} \\ &= 2^{n+2} - 2 \times (2-1)^{n+1} = 2^{n+2} - 2. \end{aligned}$$

□

4 补充 4 设 $f(x) \in \mathbb{F}_p[x]$, $\deg f = p-2$. 若对所有 $\alpha \in \mathbb{F}_p \, (\alpha \neq 0)$ 有 $f(\alpha) = \alpha^{-1}$, 试确定 $f(x)$.

证明. 由题设知 $1, 2, \ldots, p-1$ 是 $xf - 1$ 的根, 而 $xf-1$ 是 $p-1$ 次多项式, 因此

$$xf - 1 = a \prod_{\alpha=1}^{p-1} (x - \alpha) = a(x^{p-1} - 1),$$

而 $xf - 1$ 常数项为 -1, 因此 $a = 1$, $f(x) = x^{p-2}$. □

5 补充 (1) 求有理系数多项式 $\alpha(x)$ 和 $\beta(x)$, 使得

$$x^3 \alpha(x) + (1-x)^2 \beta(x) = 1.$$

(2) 求有理系数多项式 $\alpha(x)$ 和 $\beta(x)$, 使得

$$x^m \alpha(x) + (1-x)^n \beta(x) = 1,$$

其中 m, n 为正整数.

证明. 利用辗转相除法,

$$x^3 = (x+2)(1-x)^2 + 3x - 2,$$

$$(1-x)^2 = (3x-4)(3x-2)/9 + 1/9,$$

于是

$$\begin{aligned}1&=9(1-x)^2-(3x-4)(3x-2)\\&=9(1-x)^2-(3x-4)(x^3-(x+2)(1-x)^2)\\&=(4-3x)x^3+(3x^2+2x+1)(1-x)^2.\end{aligned}$$

因此取 $\alpha(x)=4-3x,\beta(x)=3x^2+2x+1$ 即可.

(2) 由

$$(1-x^m)^n=(1-x)^n(\frac{x^m-1}{x-1})^n=1+\sum_{k=1}^{n}\binom{n}{k}(-1)^k x^{km}$$

知可取

$$\alpha(x)=\sum_{k=0}^{n-1}\binom{n}{k+1}(-1)^k x^{km},\beta(x)=(\frac{x^m-1}{x-1})^n.$$ □

6 补充 1 设 $f(x)\in\mathbb{R}[x]$ 是实系数多项式, $a\in\mathbb{R}$. 假设 $f^{(n)}(a)\neq 0,\forall n$, 试决定 a 在下述多项式的零点重数:

(1) $f(x)-f(a)-f'(a)(x-a)-\frac{f''(a)}{2}(x-a)^2$;

(2) $f(x)-f(a)-\frac{x-a}{2}(f'(x)+f'(a))$.

6 补充 2 设 $n\geqslant 2$. 证明 1 是多项式 $x^{2n}-nx^{n+1}+nx^{n-1}-1$ 的 3 重零点.

6 补充 3 证明多项式 $f(x)=\sum\limits_{k=0}^{n}\dfrac{x^k}{k!}$ 无重根.

9 补充 证明

$$f_n(x)=\frac{1}{n}\sum_{d|n}\mu(d)x^{n/d}$$

为整值多项式, 其中 μ 是 Mobiüs 函数.

证明. 设 $g_n(x)=nf_n(x)\in\mathbb{Z}[x]$. 当 $n=1$ 时, $f_1(x)=x$ 显然成立. 假设 $f_1,\dots,f_{n-1}$ 均是整值多项式. 设 $n=p^\alpha n'$, $p\nmid n'$, 则

$$\begin{aligned}g_n(x)&=\sum_{d|n}\mu(d)x^{n/d}\\&=\sum_{d|n'}\mu(d)x^{p^\alpha n'/d}+\sum_{d'|n'}\mu(d'p)x^{p^{\alpha-1}n'/d'}\\&=g_{n'}(x^{p^\alpha})-g_{n'}(x^{p^{\alpha-1}}).\end{aligned}$$

而 $x\in\mathbb{Z}$ 时,

$$p^\alpha\mid x^{p^\alpha}-x^{p^{\alpha-1}}\mid g_{n'}(x^{p^\alpha})-g_{n'}(x^{p^{\alpha-1}}),$$

因此 $p^\alpha\mid g_n(x)$. 又由归纳假设 $n'\mid g_{n'}(x)$, 因此 $n\mid g_n(x)$. □

8 补充 设 R 是含幺交换环. 试定义 Euler 函数并陈述 Euler 定理, Wilson 定理, 二次剩余.

解. 设 $I \subseteq R$ 为一理想. 定义

$$\varphi(I) = |(R/I)^\times| \in \mathbb{N} \cup \{\infty\}.$$

当 $\varphi(I)$ 有限时, 若 $a \in R$ 在 R/I 中的像 $\bar{a}$ 可逆, 则

$$a^{\varphi(I)} \equiv 1 \mod I.$$

当 I 为极大理想且 $\varphi(I)$ 有限时, R/I 为有限域, 于是

$$\prod_{0 \neq x \in R/I} x = -1.$$

此时若 $\varphi(I)$ 为偶数, 则 $(R/I)^\times$ 为 $\varphi(I)$ 阶循环群, 不妨设 a 为一生成元 (原根), 则 $(R/I)^\times$ 中的平方元一定具有形式 a^{2k}, 这意味着 $a^{\varphi(I)/2} = 1$; $(R/I)^\times$ 中的非平方元一定具有形式 a^{2k+1}, 这意味着 $a^{\varphi(I)/2} = -1$. □

令 $R = \mathbb{Z}[x]$, $I = (p, \alpha(x))$, 其中 p 为素数, $\bar{\alpha} = \alpha \mod p$ 为 $\mathbb{F}_p[x]$ 中 n 次多项式. 则

$$R/I \cong \mathbb{F}_p[x]/(\bar{\alpha}) \cong \prod_i \mathbb{F}_{p^{n_i}}$$

为整环, 其中 n_i 为 $\bar{\alpha}$ 的各个不可约多项式因子 β_i 的次数. 故

$$\varphi(I) = \prod_i (p^{n_i} - 1),$$

此即群 $(R/I)^\times$ 的阶, 由此可得重模的 Euler 定理:

设 $f(x) \in \mathbb{Z}[x]$ 满足 $\bar{f}$ 与 $\bar{\alpha}$ 在 $\mathbb{F}_p[x]$ 中互素, 则

$$f(x)^{\varphi((p,\alpha))} \equiv 1 \bmod \alpha.$$

8 设 $\psi(x)$ 及 $\varphi(x)$ 都是 $\mod p$ 不可约多项式. 证明重模 $(p, \varphi(x))$ 方程 $\psi(X) \equiv 0$ 有解当且仅当 $\deg \psi \mid \deg \varphi$, 且此时 $\psi(x)$ 可分解为一次因子之积.

证明. 我们固定 $\mathbb{Z}[x]/(p, \varphi(x)) \cong \mathbb{F}_{p^n}$. 由于 $\psi(x)$ 在 $\mathbb{F}_p$ 上不可约, 由有限域基本理论知其在 $\mathbb{F}_{p^n}$ 上可解当且仅当 $m = \deg \psi \mid n$, 且此时所有根均落在 $\mathbb{F}_{p^m}$ 上. □

10 补充 若 $f(x)$ 对重模 $(p, \varphi(x)$ 的次数为 ℓ, 则 $\ell \mid p^n - 1$, 其中 n 为 $\varphi(x)$ 的次数.

证明. 由有限循环群的结构可知. □

第五章 素数分布之概况

4.1 若不然, 设 $p_1,\dots,p_m$ 为所有 $6n-1$ 型素数. 令 $N=6p_1\cdots p_m-1$, 则 $2,3,p_i$ 均不整除 N, 因此 N 只含有 $6n+1$ 型素数. 但是 $6n+1$ 型素数乘积一定为 $6n+1$ 型, 这与 N 是 $6n-1$ 型矛盾! 因此有无穷多 $6n-1$ 型素数.

4.2 若不然, 设 $p_1,\dots,p_m$ 为所有 $4n-1$ 型素数. 令 $N=4p_1\cdots p_m-1$, 则 $2,p_i$ 均不整除 N, 因此 N 只含有 $4n+1$ 型素数. 但是 $4n+1$ 型素数乘积一定为 $4n+1$ 型, 这与 N 是 $4n-1$ 型矛盾! 因此有无穷多 $4n-1$ 型素数.

4.3 由

$$\begin{aligned}\frac{\pi^2}{6}&=\sum_{n=1}^{\infty}\frac{1}{n^2}\\&=\prod_p(1+p^{-2}+p^{-4}+\cdots)\\&=\prod_p(1-p^{-2})^{-2}\\&=\prod_p\frac{p^2}{p^2-1}\end{aligned}$$

可得.

remark 此即 Riemann ζ 函数在 2 处的取值, 一般地

$$\zeta(2n)=\frac{(-1)^{n+1}B_{2n}(2\pi)^{2n}}{2(2n)!},\quad n\geqslant 1,$$

这里 B_n 是 Bernoulli 数, 即

$$\frac{t}{e^t-1}=\sum_{m=0}^{\infty}B_m\frac{t^m}{m!}.$$

remark

7 令 $x=\sqrt{2n}>0$, 原式等价于

$$2^{x^2/3}<x^{2(x+1)}$$

$$\frac{1}{6}x^2\ln 2<(x+1)\ln x.$$

令 $f(x)=(x+1)\ln x-\frac{1}{6}x^2\ln 2$, 则

$$\begin{aligned}f'(x)&=\ln x+\frac{x+1}{x}-\frac{\ln 2}{3}x,\\f''(x)&=\frac{1}{x}-\frac{1}{x^2}-\frac{\ln 2}{3},\\f'''(x)&=-\frac{1}{x^2}+\frac{2}{x^3}.\end{aligned}$$

由于 $x<2$ 时 $f'''(x)>0$; $x>2$ 时 $f'''(x)<0$, 因此 $f''(x)$ 在 $(0,2)$ 上单调增, 在 $(2\ +\infty)$ 上单调减.

由

$$f''(1)=-\frac{\ln 2}{3}<0,\ f''(2)=\frac{1}{4}-\frac{\ln 2}{3}>0,\ f''(3)=\frac{2}{9}-\frac{\ln 2}{3}<0$$

知 $f''(x)$ 在 $(0,+\infty)$ 上恰有两个零点 $1<x_1<2<x_2<3$. 因此 $f'(x)$ 在 $(0,x_1)$ 和 $(x_2,+\infty)$ 上单调减; 在 (x_1,x_2) 上单调增.

由于 $0<x<3$ 时

$$f'(x)\geqslant\frac{4}{3}-\ln 2>0,$$

因此 $f'(x)$ 恰有一个零点 $x_3>3$. 故 $f(x)$ 在 $(0,x_3)$ 上单调增, 在 $(x_3,+\infty)$ 上单调减.

由于

$$f(\sqrt{2})=\frac{3\sqrt{2}+1}{6}\ln 2>0,$$

$$f(\sqrt{2\times 467})\approx 0.032>0,\ f(\sqrt{2\times 468})\approx -0.054<0,$$

因此当且仅当 $1\leqslant n\leqslant 467$ 时, $f(\sqrt{2n})>0$.

8.1 分别将 ξ 和 $\xi+1$ 代入并相减得

$$(\xi+1)^\lambda=\frac{(\xi+1)^{\lambda+1}-\xi^{\lambda+1}}{\lambda+1}+c((\xi+1)^\lambda-\xi^\lambda)+O(\xi^{\lambda-2}),$$

化简可得 $c=1/2$.

8.2 由

$$\int\log\log x\,\mathrm{d}x=x\log\log x-\operatorname{li}x$$

知

$$\sum_{3\leqslant 3\leqslant\xi}\log\log n=\int_3^\xi\log\log x\,\mathrm{d}x+O(\log\log\xi)$$

$$=\xi\log\log\xi-\operatorname{li}\xi+O(\log\log\xi)=\xi\log\log\xi+O(\frac{\xi}{\log\xi}).$$

8.1' 令 $f(x)=\frac{\log x}{x}$, 则

$$f'(x)=\frac{1-\log x}{x^2},$$

因此 $x\geqslant 3$ 时 $f'(x)<0$, $f(x)$ 单调减且趋于 0. 由定理 2 知

$$\lim_{N\to\infty}(\sum_{n=3}^N f(n)-\int_3^N f(x)\,\mathrm{d}x)=\alpha$$

存在, 且

$$|\sum_{3\leqslant n\leqslant\xi}f(n)-\int_3^\xi f(x)\,\mathrm{d}x-\alpha|\leqslant f(\xi-1)=O(f(\xi)),$$

即
$$\sum_{3\leqslant n\leqslant\xi} f(n)=\int_3^{\xi} f(x)\,\mathrm{d}x+\alpha+O(f(\xi)).$$
由 $\int f(x)\,\mathrm{d}x=\frac{1}{2}\log^2 x$ 知
$$\sum_{1\leqslant n\leqslant\xi}\frac{\log n}{n}=\frac{1}{2}\log^2\xi-\frac{1}{2}\log^2 3+\frac{\log 2}{2}+\alpha+O(\frac{\log\xi}{\xi}).$$
8.2’ 令 $f(x)=\frac{1}{x\log x}$, 则
$$f'(x)=-\frac{1+\log x}{(x\log x)^2},$$
因此 $x\geqslant 2$ 时 $f'(x)<0$, $f(x)$ 单调减且趋于 0. 由定理 2 知
$$\lim_{N\to\infty}(\sum_{n=2}^{N} f(n)-\int_2^{N} f(x)\,\mathrm{d}x)=\alpha$$
存在, 且
$$|\sum_{2\leqslant n\leqslant\xi} f(n)-\int_2^{\xi} f(x)\,\mathrm{d}x-\alpha|\leqslant f(\xi-1)=O(f(\xi)),$$
即
$$\sum_{2\leqslant n\leqslant\xi} f(n)=\int_2^{\xi} f(x)\,\mathrm{d}x+\alpha+O(f(\xi)).$$
由 $\int f(x)\,\mathrm{d}x=\log\log x$ 知
$$\sum_{2\leqslant n\leqslant\xi}\frac{1}{n\log n}=\log\log\xi-\log\log 2+\alpha+O(\frac{1}{\xi\log\xi}).$$
9.1 由 Чебыщев 定理知
$$\frac{1}{8}\leqslant\frac{n\log p_n}{p_n}\leqslant 12,$$
因此
$$\frac{p_n}{n\log n}>\frac{p_n}{n\log p_n}\geqslant c_1=\frac{1}{12}.$$
由于 $\log p_n<2\sqrt{p_n}$,
$$\frac{1}{8}\leqslant\frac{n\log p_n}{p_n}<\frac{2n}{\sqrt{p_n}},$$
$$\log n>\frac{1}{2}\log p_n-\log 16,$$
$$\frac{n\log n}{p_n}>\frac{1}{2}\frac{n\log p_n}{p_n}-\frac{n\log 16}{p_n}\geqslant\frac{1}{16}-\frac{12\log 16}{\log p_n}.$$
设素数 $p_k>16^{192}$, 则 $n\geqslant k$ 时上式 $\geqslant\frac{\log(p_k/16^{192})}{16\log p_k}>0$.

令

$$c_0 = \min\{\frac{2\log 2}{p_2}, \dots, \frac{(k-1)\log(k-1)}{p_{k-1}}, \frac{\log(p_k/16^{192})}{16\log p_k}\},$$

$c_2 = 2/c_0$, 则

$$c_1 n\log n < p_n < c_2 n\log n.$$

9.2 设 $n = \prod\limits_{i=1}^{k} q_i^{e_i}$, 令

$$f(n) = \frac{\varphi(n)\log\log n}{n} = \log(\sum e_i \log q_i)\prod(1-\frac{1}{q_i}).$$

设 $k \geqslant 2$, 则 $n \geqslant 3$. 记 p_i 为第 i 个素数, 则

$$f(n) \geqslant \log(\sum \log p_i)\prod(1-\frac{1}{p_i}).$$

由 Stirling 公式, 存在 $c_0 > 0$ 使得 $n! > c_0(n/e)^n$, 于是

$$p_1\cdots p_k > k! > c_0(k/e)^k,$$

$$f(n) \geqslant \log(k\log(k/e) + \log c_0)\prod(1-\frac{1}{p_i}).$$

当 n 充分大时, 存在 $c_1 > 0$ 使得 $f(n) \geqslant c_1 \log k/\log p_k \geqslant c > 0$.
$k = 1$ 时易得 $f(n) \geqslant \min\{f(3), f(4)\}$.

9.3 由

$$\sum_p \frac{1}{p(\log\log p)^h}$$

和

$$\sum_{n\geqslant 1} \frac{1}{n\log n(\log\log n)^h}$$

相互控制可得, 而它的敛散性和

$$\int_a^{+\infty} \frac{\mathrm{d}x}{x\log x(\log\log x)^h} = \int_{\log\log a}^{+\infty} \frac{\mathrm{d}t}{t^h}$$

相同.

11.1 设 $c \in \mathbb{Z}$ 满足 $|f(c)| \geqslant 2$, 设

$$g(x) = f(x+c) = a_n x^n + \cdots + a_1 x + f(c),$$

则

$$g(mf(c)) = (\sum_{i=1}^{n} a_i m^i f(c)^{i-1} + 1)f(c),$$

当 m 充分大时 $f(mf(c)+c) = g(mf(c))$ 是合数.

11.2 设

$$f(n)=c_1(n)+c_2(n)2^n+\cdots+c_m(n)m^n.$$

若不然, 存在 $f(a)=p>m$. 由

$$f(a+p(p-1)t)\equiv f(a) \bmod p$$

知 $p\mid f(a+p(p-1)t)$. 由 $n\to\infty$ 时 $f(n)\to\infty$ 可知存在无穷多 t 使得 $f(a+p(p-1)t)$ 是复合数.

12 若素数 $p\mid x^2+y^2, xy\neq 0$, 则 $-1\equiv (x/y)^2 \bmod p$, 因此 $\left(\frac{-1}{p}\right)=1, p\equiv 1 \bmod 4$.

若只有有限个 $8n+5$ 型素数, 设为 $p_1,\dots,p_k$, 令

$$q=(p_1\cdots p_k)^2+2^2,$$

则 $p_i\nmid q$, 因此 q 只含 $8n+1$ 型素因子, 从而 $q\equiv 1 \bmod 8$, 这与 $q\equiv 5 \bmod 8$ 矛盾.

第六章　数论函数

4.1 由第二章 5 补充 3 知

$$g*f_1=(f*E_0)*f_1=f*(f_1*E_0)=f*g_1.$$

4.2 由于

$$g(e)g_1(e)=\sum_{d,d_1\mid e} f(d)f_1(d_1),$$

因此 gg_1 的 Möbius 变换为

$$\begin{aligned}h(n)&=\sum_{d,d_1\mid e\mid n} f(d)f_1(d_1)\mu(\frac{n}{e})\\&=\sum_{d,d_1\mid n} f(d)f_1(d_1)\sum_{f\mid \frac{n}{[d,d_1]}}\mu(\frac{n}{f[d,d_1]})\\&=\sum_{[d,d_1]=n} f(d)f_1(d_1)\end{aligned}$$

4.3 由

$$(E_0*E_0)(n)=\sum_{d\mid n}E_0(d)E_0(\frac{n}{d})=d(n)$$

立得.

5.1 我们有

$$\sum_{1\leqslant n\leqslant\xi}\frac{d(n)}{n}=\sum_{1\leqslant n\leqslant\xi}\sum_{u|n}\frac{1}{n}=\sum_{1\leqslant uv\leqslant\xi}\frac{1}{uv}.$$

该区域可分为 $(0,\sqrt{\xi}]^2$ 和其余两块, 于是

$$\begin{aligned}
&\sum_{1\leqslant uv\leqslant\xi}(uv)^{-1}\\
=&(\sum_{1\leqslant u\leqslant\sqrt{\xi}}u^{-1})^2+2\sum_{1\leqslant u\leqslant\sqrt{\xi}}u^{-1}\sum_{\sqrt{\xi}<v\leqslant\xi/u}v^{-1}\\
=&-(\sum_{1\leqslant u\leqslant\sqrt{\xi}}u^{-1})^2+2\sum_{1\leqslant u\leqslant\sqrt{\xi}}u^{-1}\sum_{1\leqslant v\leqslant\xi/u}v^{-1}\\
=&\sum_{1\leqslant u\leqslant\sqrt{\xi}}u^{-1}(2\sum_{1\leqslant v\leqslant\xi/u}v^{-1}-\sum_{1\leqslant v\leqslant\sqrt{\xi}}v^{-1})\\
=&\sum_{1\leqslant u\leqslant\sqrt{\xi}}u^{-1}(2\log\xi-2\log u+2\gamma-\frac{1}{2}\log\xi-\gamma+O(\xi^{-\frac{1}{2}}))\\
=&-2\sum_{1\leqslant u\leqslant\sqrt{\xi}}\frac{\log u}{u}+(\log\sqrt{\xi}+\gamma+O(\xi^{-\frac{1}{2}}))(\frac{3}{2}\log\xi+\gamma+O(\xi^{-\frac{1}{2}}))\\
=&-2(\frac{1}{2}\log^2\sqrt{\xi}+c_1+O(\xi^{-\frac{1}{2}}\log\xi))+\frac{3}{4}\log^2\xi+2\gamma\log\xi+O(\xi^{-\frac{1}{2}}\log\xi)\\
=&\frac{1}{2}\log^2\xi+2\gamma\log\xi+c+O(\xi^{-\frac{1}{2}}\log\xi).
\end{aligned}$$

5.2 由

$$\sigma(n)=\prod\frac{p^{e+1}-1}{p-1}=\prod O(p^{e(1+\varepsilon)})=n^{1+\varepsilon}$$

可得.

5.3 令

$$b_v=\sum_{1\leqslant u\leqslant\xi/v}u=\frac{\xi^2}{2v^2}+(1-2\lambda_v)\frac{\xi}{v}+\lambda_v(\lambda_v-1),$$

其中 $\lambda_v=\frac{\xi}{v}-[\frac{\xi}{v}]$, 则

$$\begin{aligned}
&\sum_{1\leqslant n\leqslant\xi}\sigma(n)=\sum_{1\leqslant n\leqslant\xi}\sum_{u|n}u=\sum_{1\leqslant uv\leqslant\xi}u=\sum_{1\leqslant u\leqslant\xi}u[\frac{\xi}{u}]\\
=&\sum_{1\leqslant v\leqslant\xi}v(b_v-b_{v+1})=\sum_{1\leqslant k\leqslant\xi}b_k-[\xi]b_{[\xi]}\\
=&\frac{\xi^2}{2}\sum_{1\leqslant k\leqslant\xi}\frac{1}{v^2}+O(\xi\log\xi)=\frac{\xi^2\pi^2}{12}+O(\xi\log\xi).
\end{aligned}$$

9.1 设椭圆的长轴和短轴长为 $2a,2b$, 则由定理 2 及 $A=\pi ab$, $l\leqslant 2\pi(a+b)$ 得 $N=\pi ab+O(a+b)$.

9.2 该数为

$$\begin{aligned}&\sum_{w^2\leqslant x}(\pi(x-w^2)+O(\sqrt{x-w^2}))\\=&\pi x(2[\sqrt{x}]+1)-\pi\frac{[\sqrt{x}]([\sqrt{x}]+1)(2[\sqrt{x}]+1)}{3}+O(x)\\=&\frac{4}{3}\pi x^{3/2}+O(x).\end{aligned}$$

9.3 假设 n 维球 $x_1^2+\cdots+x_n^2\leqslant x$ 内整点个数为

$$f_n=c_nx^{\frac{n}{2}}+O(x^{\frac{n-1}{2}}),$$

则

$$\begin{aligned}f_{n+1}=&\sum_{w^2\leqslant x}(c_n(x-w^2)^{\frac{n}{2}}+O((x-w^2)^{\frac{n-1}{2}}))\\=&2c_nd_nx^{\frac{n+1}{2}}+O(x^{\frac{n}{2}}),\end{aligned}$$

其中

$$\begin{aligned}d_n&=1-\binom{n/2}{1}\frac{1}{3}+\binom{n/2}{2}\frac{1}{5}-\binom{n/2}{3}\frac{1}{7}+\cdots\\&=\int_0^1(1-x^2)^{n/2}\,\mathrm{d}x=\frac{\sqrt{\pi}\Gamma(\frac{n+2}{2})}{2\Gamma(\frac{n+3}{2})},\end{aligned}$$

因此由数学归纳法

$$c_n=\pi\prod_{k=2}^{k-1}\frac{\sqrt{\pi}\Gamma(\frac{k+2}{2})}{\Gamma(\frac{k+3}{2})}=\frac{\pi^{\frac{n}{2}}}{\Gamma(\frac{n}{2}+1)},$$

$$f_n=\frac{(\pi x)^{\frac{n}{2}}}{\Gamma(\frac{n}{2}+1)}+O(x^{\frac{n-1}{2}}).$$

注 6.1. 由此可知半径为 r 的 n 维球的体积为 $\frac{\pi^{n/2}r^n}{\Gamma(\frac{n}{2}+1)}$.

9.4 我们有

$$\begin{aligned}\sum_{1\leqslant n\leqslant x}r^2(x)&=16\sum_{\substack{1\leqslant n\leqslant x\\d_1,d_2\mid n}}\chi(d_1d_2)\\&=16\sum_{1\leqslant d_1,d_2\leqslant x}\chi(d_1d_2)[\frac{x}{[d_1,d_2]}]\\&=16\sum_{1\leqslant s\leqslant x}\sum_{\substack{1\leqslant u,v\leqslant x/s\\(u,v)=1}}\chi(s^2uv)[\frac{x}{suv}]\\&=16\sum_{1\leqslant s\leqslant x}\chi(s^2)\sum_{1\leqslant t\leqslant x/s}\chi(t)[\frac{x}{st}]d(t)\\&=16\sum_{1\leqslant s\leqslant x}\chi(s^2)f(x/s)\end{aligned}$$

其中

$$\begin{aligned}f(x) &= \sum_{1\leqslant t\leqslant x}\chi(t)[\frac{x}{t}]d(t)\\ &= x\prod_{1\leqslant p\leqslant x}(1-\chi(p)p^{-1})^{-2}+O(\log x)\\ &= x(\prod_{n\geqslant 1}\frac{\chi(n)}{n})^2+O(\log x)\\ &= \frac{\pi^2 x}{16}+O(\log x),\end{aligned}$$

因此

$$\begin{aligned}\sum_{1\leqslant n\leqslant x}r^2(x) &= 16\sum_{1\leqslant s\leqslant x}\chi(s^2)f(x/s)\\ &= \pi^2 x\sum_{1\leqslant t\leqslant \frac{x+1}{2}}\frac{1}{2t-1}+O(\log x)\\ &= \pi^2 x(\log x-\frac{1}{2}\log x)+O(x)\\ &= \frac{\pi^2 x\log x}{2}+O(x).\end{aligned}$$

9.5 令

$$s(x)=\sum_{1\leqslant n\leqslant x}r(n),$$

则要求的数为

$$\begin{aligned}&\sum_{1\leqslant d\leqslant\sqrt{x}}s(x/d^2)\mu(d)\\ =&\sum_{1\leqslant d\leqslant\sqrt{x}}(\frac{\pi x}{d^2}+O(\frac{\sqrt{x}}{d}))\mu(d)\\ =&\pi x(\prod_{1\leqslant p\leqslant\sqrt{x}}(1-p^{-2}))+O(\sqrt{x}\prod_{1\leqslant p\leqslant\sqrt{x}}(1-p^{-1}))\\ =&\frac{6}{\pi}x+O(\sqrt{x}\log x).\end{aligned}$$

参考文献

[冯] 冯克勤, 余红兵, 整数与多项式, 高等教育出版社, 施普林格出版社, 1999
[华] 华罗庚, 华罗庚文集数论卷 *II*, 科学出版社, 2010
[欧阳] 欧阳毅, 代数学基础, 中国科学技术大学

E-mail address: zsxqq@mail.ustc.edu.cn