《初等数论及其应用》参考答案

兰州大学　数学与统计学院　李宇航

写在前面

本文档是冯克勤编著的《初等数论及其应用》的参考答案，兰州大学数学与统计学院数论课程使用的是这本教材，笔者在学习时，常常感到力不从心，其他许多同学也有此想法，对课后的习题难以下笔，而书中的参考答案仅有部分，因此笔者产生了编写这本书全部答案的想法，从大一下 2 月份开始，直到 6 月，历经大约一学期的时间完成了编写，在此期间受到了贾星星老师的帮助，以及许多同学的支持与鼓励，在此感谢。

数论是一门研究整数性质的数学分支，是一门很有趣的课程。引用冯克勤前辈在《初等数论及其应用》前言中说的话，“我最基本的想法是想通过本书使读者感受到数论是有趣，也是有用的，但不知能否有这样的效果，欢迎批评指正”，编写此答案，是希望更多的人能够更好的进入到数论的学习，完成习题的过程中能够订正与参考，体会到数论虽然艰涩但亦可琢磨。同时，希望大家不要一味的抄袭答案，这是与我编写此答案的初衷背道而驰的。除此之外，也希望同学们在除“标准答案”之外也有自己的想法，更好的想法，不光是在数论的学习之路上进步，也在数学之路上逐渐成长，看待数学有自己的理解。

笔者能力有限，时间也较为紧迫，有些地方难免出错，请各位读者不吝批评指正。

李宇航

2023 年 6 月 18 日于兰州大学

联系方式:

邮箱: liyuhang21@lzu.edu.cn

QQ: 2840317849

目录

1 数的整除性

1.1 整除性

1. 设 n 是奇数, 则 $8 \mid n^2 - 1$.

解答.

设 $n = 2k - 1,\ k = 1, 2, \cdots, n$

那么 $n^2 - 1 = 4k^2 - 4k = 4k(k-1)$

$k = 1$ 时, $8 \mid 0$, 结论成立

$k > 1$ 时, $k,\ k-1$ 奇偶性不同, 故 $2 \mid k(k-1)$, 进而 $8 \mid 4k(k-1)$, 即 $8 \mid n^2 - 1$

2. 设 $n \geq 3$ 是奇数, 证明: $\left(1 + \frac{1}{2} + \cdots + \frac{1}{n-1}\right)(n-1)!$ 被 n 整除.

解答.

注意到

$$\begin{aligned} 2\left(1 + \frac{1}{2} + \cdots + \frac{1}{n-1}\right)(n-1)! &= \sum_{k=1}^{n}\left(\frac{1}{k} + \frac{1}{n-k}\right)(n-1)! \\ &= n\sum_{k=1}^{n}\frac{(n-1)!}{k(n-k)} \end{aligned}$$

这说明 $n \mid 2\left(1 + \frac{1}{2} + \cdots + \frac{1}{n-1}\right)(n-1)!$

因为 n 为奇数, 所以 $(2, n) = 1$, 进而 $n \mid \left(1 + \frac{1}{2} + \cdots + \frac{1}{n-1}\right)(n-1)!$

3. 设 m 和 n 是正整数, $m \geq 3$. 证明: $2^m - 1 \nmid 2^n + 1$.

解答.

若 $m > n$, 那么 $2^m - 1 > 2^m + 1$, 故 $2^m - 1 \nmid 2^n + 1$

若 $m \leq n$, 做带余除法有 $n = qm + r,\ 0 \leq r < m$, 进而

$$2^n + 1 = 2^{qm+r} + 1 = (2^m - 1)\sum_{k=0}^{q-1} 2^{km+r} + (2^r + 1)$$

若 $2^m - 1 \mid 2^n + 1$, 那么根据上式必然有 $2^m - 1 \mid 2^r + 1$

而 $2^m - 1 \geq 2^{r+1} - 1 \geq 2^r + 1$, 矛盾!

故 $2^m - 1 \nmid 2^n + 1$

4. 设 q 是大于 1 的整数. 证明:
(i)每个正整数 n 可以惟一地表示成

$$n = a_0 + a_1 q + a_2 q^2 + \cdots + a_k q^k,$$

其中 a_i 是满足 $0 \le a_i \le q-1$ 的整数 $(0 \le i \le k)$, 并且 $a_k \ne 0$. 这叫做 n 的 q 进制表示.
(ii)$a_i = \left[\dfrac{n}{q_i}\right] - q\left[\dfrac{n}{q^{i+1}}\right] (0 \le i \le k)$.

解答.
(i)先证明存在性,
$n=1$ 时, 其 q 进制表示为 1
假设 $n = a_0 + a_1 q + a_2 q^2 + \cdots + a_k q^k$, 那么 $n+1 = 1 + a_0 + a_1 q + a_2 q^2 + \cdots + a_k q^k$
若 $a_0 + 1 \le q-1$, 结论已经成立
若 $a_0 + 1 = q$, 那么只需将 $a_0 + 1$ 合并到 $a_1 q$ 这一项上, 依次考虑合并后系数与 $q-1$ 的关系, 若系数小于等于 $q-1$, 则无需做出改变; 若系数等于 q, 只需依次向后合并即可
故 $n+1$ 也存在 q 进制表示
再证明唯一性
设 n 还存在 q 进制表达式 $n = b_0 + b_1 q + b_2 q^2 + \cdots + b_s q^s$
若 $s > k$, 那么 $n = a_0 + a_1 q + a_2 a^2 + \cdots + a_k q^k \le (q-1)\left(1 + q + q^2 + \cdots + q^k\right) = q^k - 1 < q^s \le n$, 矛盾! 故 $s \le k$, 同理 $s \ge k$, 进而 $s = k$, 设 l 是使得 a_l与 b_l 不相等的最大正整数, 不妨设 $a_l > b_l$, 那么 $q^l > (q-1)\left(1 + q + \cdots + q^{l-1}\right) > b_0 + b_1 q + \cdots + b_{l-1} q^{l-1}$. 这说明 $n = \sum\limits_{i=0}^{k} a_i q^i > \sum\limits_{i=0}^{s} b_i q^i = n$, 矛盾! 因此存在唯一的 q 进制表达式
(ii)根据系数的唯一性, 只验证即可

$$\begin{aligned}
\sum_{i=0}^{k} a_i q^i &= \sum_{i=0}^{k} \left(\left[\frac{n}{q_i}\right] - q\left[\frac{n}{q^{i+1}}\right]\right) q^i \\
&= [n] - q^{k+1}\left[\frac{n}{q^{k+1}}\right] \\
&= n
\end{aligned}$$

5. 设 $\alpha_1, \cdots, \alpha_2$ 为实数 $(n \ge 2)$, 证明:

$$[\alpha_1] + [\alpha_2] + \cdots + [\alpha_n] \le [\alpha_1 + \alpha_2 + \cdots + \alpha_n] \le [\alpha_1] + [\alpha_2] + \cdots + [\alpha_n] + n - 1.$$

解答.

注意到

$$
\begin{aligned}
[\alpha_1+\alpha_2+\cdots+\alpha_n] &= [[\alpha_1]+[\alpha_2]+\cdots+[\alpha_n]+\{\alpha_1\}+\{\alpha_2\}+\cdots+\{\alpha_n\}] \\
&= [\alpha_1]+[\alpha_2]+\cdots+[\alpha_n]+[\{\alpha_1\}+\{\alpha_2\}+\cdots+\{\alpha_n\}]
\end{aligned}
$$

因为

$$0 \leq \{\alpha_1\}+\{\alpha_2\}+\cdots+\{\alpha_n\} < n$$

进而

$$0 \leq [\{\alpha_1\}+\{\alpha_2\}+\cdots+\{\alpha_n\}] \leq n-1$$

故

$$[\alpha_1]+[\alpha_2]+\cdots+[\alpha_n] \leq [\alpha_1+\alpha_2+\cdots+\alpha_n] \leq [\alpha_1]+[\alpha_2]+\cdots+[\alpha_n]+n-1.$$

6. 设 α 和 β 为实数,证明: $[2\alpha]+[2\beta] \geq [\alpha]+[\beta]+[\alpha+\beta]$.

解答.

设 $f(\alpha,\beta)=[2\alpha]+[2\beta]-[\alpha]-[\beta]-[\alpha+\beta]$, 即证 $f(\alpha,\beta) \geq 0$

注意到

$$
\begin{aligned}
f(\alpha+1,\beta) &= [2\alpha+2]+[2\beta]-[\alpha+1]-[\beta]-[\alpha+\beta+1] \\
&= [2\alpha]+2+[2\beta]-[\alpha]-1-[\beta]-[\alpha+\beta]-1 \\
&= [2\alpha]+[2\beta]-[\alpha]-[\beta]-[\alpha+\beta] \\
&= f(\alpha,\beta)
\end{aligned}
$$

由于 $f(\alpha,\beta)=f(\beta,\alpha)$, 故也有 $f(\alpha,\beta+1)=f(\alpha,\beta)$, 那么只需在 α, $\beta \in [0,1)$ 上证明即可

此时, $f(\alpha,\beta)=[2\alpha]+[2\beta]-[\alpha+\beta]$

当 $\alpha+\beta \in (0,1]$ 时

$$f(\alpha,\beta)=[2\alpha]+[2\beta] \geq 0$$

当 $\alpha+\beta \in [1,2)$时, $\max\{\alpha,\beta\} \geq \dfrac{\alpha+\beta}{2} \geq \dfrac{1}{2}$, 进而 $\max\{[2\alpha],[2\beta]\} \geq 1$, 故

$$f(\alpha,\beta)=[2\alpha]+[2\beta]-1 \geq 1-1=0$$

故原不等式成立

7. 设 x 为实数, $n \geq 2$ 为整数, 证明:

$$[x]+\left[x+\frac{1}{n}\right]+\cdots+\left[x+\frac{n-1}{n}\right]=[nx]$$

解答.

记 $f(x)=[x]+\left[x+\frac{1}{n}\right]+\cdots+\left[x+\frac{n-1}{n}\right]-[nx]$, $x \in \mathbb{R}$, 即证 $f(x) \equiv 0$

注意到

$$\begin{aligned} f\left(x+\frac{1}{n}\right) &= \left[x+\frac{1}{n}\right]+\left[x+\frac{2}{n}\right]+\cdots+[x+1]-[nx+1] \\ &= \left[x+\frac{1}{n}\right]+\left[x+\frac{2}{n}\right]+\cdots+[x]+1-[nx]-1 \\ &= f(x) \end{aligned}$$

故只需证明 $x \in \left[0, \frac{1}{n}\right)$ 时的情况, 此时 $x+\frac{k}{n} \in [0,1)$, $nx \in [0,1)$, 故 $f(x) \equiv 0$

8. 对正整数 m 和素数 p, 我们用 $p^e \| m$ 表示" $p^e \mid m$, 但是 $p^{e+1} \nmid m$". 设 n 为正整数, $p^e \| n!$. 证明:

(i)$e=\sum_{i=1}^{\infty}\left[\frac{n}{p^i}\right]$;

(ii)对于 n 的 p 进制表示 $n=a_0+a_1 p+\cdots+a_k p^k$, 记 $S_p(n)$ 为其数字和 $a_0+a_1+\cdots+a_k$. 证明 $e=\frac{n-S_p(n)}{p-1}$.

解答.

(i)考察 $1, 2, \cdots, n$ 中能被 p^i 整除的数的个数 $n(i)$

$n(i)$ 是 $1, 2, \cdots, n$ 中 p^i 的倍数的个数, 那么 $n(i)=\left[\frac{n}{p^i}\right]$

再考察 $1, 2, \cdots, n$ 中能被 p^i 整除, 但不能被 p^{i+1} 整除的数的个数 $m(i)$, 那么 $e=\sum_{i=1}^{\infty} i m(i)$

考虑 $n(i)$ 的定义可知, $m(i)=n(i)-n(i+1)$

故

$$e=\sum_{i=1}^{\infty} i m(i)=\sum_{i=1}^{\infty} i\,(n(i)-n(i+1))=\sum_{i=1}^{\infty} n(i)=\sum_{i=1}^{\infty}\left[\frac{n}{p^i}\right]$$

(ii)一方面

$$\begin{aligned}\frac{n-S_p(n)}{p-1}&=\frac{1}{p-1}\left(\sum_{i=0}^{k}a_ip^i-\sum_{i=0}^{k}a_i\right)\\&=\sum_{i=1}^{k}a_i\frac{p^i-1}{p-1}\\&=\sum_{i=1}^{k}a_i\sum_{j=0}^{i-1}p^j\end{aligned}$$

另一方面

$$e=\sum_{i=1}^{\infty}\left[\frac{n}{p_i}\right]=\sum_{i=1}^{\infty}\left[\frac{a_0+a_1p+\cdots+a_kp^k}{p^i}\right]=\sum_{i=1}^{\infty}\left[\frac{1}{p^i}\sum_{j=0}^{i-1}a_jp^j+\frac{1}{p^i}\sum_{j=i}^{k}a_jp^j\right]$$

注意到 $0\leq\frac{1}{p_i}\sum_{j=1}^{i-1}a_jp^j\leq\frac{1}{p_i}\sum_{j=1}^{i-1}(p-1)p^j=\frac{p^i-p}{p^i}<1$, $\frac{1}{p^i}\sum_{j=i}^{k}a_jp^j=\sum_{j=i}^{k}a_jp^{j-i}$ 为整数

从而

$$e=\sum_{i=1}^{\infty}\sum_{j=i}^{k}a_jp^{j-i}=\sum_{i=1}^{k}\sum_{j=i}^{k}a_jp^{j-i}=\sum_{i=1}^{k}a_i\sum_{j=0}^{i-1}p^j$$

故 $e=\frac{n-S_p(n)}{p-1}$

9. 设 n 为整数, $n\geq 2$, 证明:

(i) $1+\frac{1}{2}+\cdots+\frac{1}{n}$ 不是整数;

(ii) $1+\frac{1}{3}+\frac{1}{5}+\cdots+\frac{1}{2n+1}$ 不是整数.

解答.

(i)设 $1+\frac{1}{2}+\cdots+\frac{1}{n}=\frac{a}{b}$, 其中 $b=\operatorname{lcm}(1,2,\cdots,n)$

因为 b 有因子 2, 所以 b 为偶数

下面考察 $a=b+\frac{b}{2}+\cdots+\frac{b}{n}$ 的奇偶性

设 $b=2^rq$, 其中 q 为奇数, 因为 $b=\operatorname{lcm}(1,2,\cdots,n)$, 设 $r\in\mathbb{Z}$ 满足 $2^r<n$ 且 $n-2^r$ 最小

故 $\frac{b}{k}\,(1\leq k\leq n)$ 为奇数当且仅当 k 中 2 的幂次也为 r, 而这样的数只有一个且为 2^r

若有多个, 不妨设这个数为 $s=2^rq_1$, q_1是大于 3 的奇数; 而 $s>2^{r+1}>n$, 矛盾!

故仅有一个 k 使得 $\frac{b}{k}$ 为奇数, 那么其余的全为偶数, 进而 a 为奇数, 那么 $\frac{a}{b}$ 一定不为整数

(ii)设 $1+\frac{1}{3}+\frac{1}{5}+\cdots+\frac{1}{2n+1}=\frac{a}{b}$, 其中 $b=\operatorname{lcm}(1,3,5,\cdots,2n+1)$

3 是 b 的因子, 故 $3\mid b$, 下面证明 $3\nmid a$, 从而 $\frac{a}{b}\notin\mathbb{Z}$

$a=b+\frac{b}{3}+\frac{b}{5}+\cdots+\frac{b}{2n+1}$, 设 $r\in\mathbb{Z}$ 满足 $3^r\leq 2n+1$ 且 $2n+1-3^r$ 最小

那么 $\dfrac{b}{k}\,(k=1,3,5,\cdots,2n+1)$ 不能被 3 整除,当且仅当 $3^r \mid k$, 于是 $k\in\{3^r, 2\cdot 3^r\}$
但 $2\cdot 3^r$ 为偶数, 不在 1, 3, 5, $\cdots$, $2n+1$之中, 故这样的数只有一个为 3^r
那么在 $\dfrac{b}{k}\,(k=1,3,5,\cdots,2n+1)$ 中只有一个不能被 3 整除, 从而 $3\nmid a$, 故 $b\nmid a$

10. 证明:(i)形如 $4m+3\,(m\in\mathbb{Z})$ 的素数有无穷多个;
(ii)形如 $6m+5\,(m\in\mathbb{Z})$ 的素数有无穷多个.

解答.
(i)反证, 设所有这样的素数从小到大排列为 $p_1, p_2, \cdots, p_k$, 置

$$P=2p_1p_2\cdots p_k+1$$

所有形如 $4m+3$ 的素数与 2 均不整除 P, 而所有素数均属于下面三类之一: 2, $4m+1$形, $4m+3$形
故 P 的素因子只有 $4m+1$ 形, 那么 P 除以 4 余 1
另一方面, 由 $P=2p_1p_2\cdots p_k+1$ 知, P 除以 4 余 3
矛盾! 进而形如 $4m+3\,(m\in\mathbb{Z})$ 的素数有无穷多个
(ii)反证, 设所有这样的素数从小到大排列为 $p_1, p_2, \cdots, p_k$, 置

$$P=3p_1p_2\cdots p_k+2$$

所有形如 $6m+5$ 的素数与 2 均不整除 P, 而所有素数均属于下面三类之一: 2, $6m+1$形, $6m+5$形
故 P 的素因子只有 $6m+1$ 形, 那么 P 除以 6 余 1
另一方面, 由 $P=3p_1p_2\cdots p_k+2$ 知 P 除以 6 余 5
矛盾! 进而形如 $6m+5(m\in\mathbb{Z})$ 的素数有无穷多个

11. 设 n 为正整数, $n\geq 2$. 如果 n 没有小于或等于 $\sqrt{n}$ 的素数因子, 则 n 为素数.

解答.
证明该命题的逆否命题, 并反证, 假设 n 存在素因子 $p\in(\sqrt{n},n]$, 那么 $p'=\dfrac{n}{p}\leq\sqrt{n}$ 也是 n 的因子, p' 的素因子都小于等于 $\sqrt{n}$, 这些素因子也是 n 的素因子, 矛盾!

12. 对每个整数 $n\geq 3$, n 和 $n!$ 之间必有素数.由此证明素数有无限多个.

解答.
反证, 假设存在 $n\geq 3$ 使得 n 和 $n!$ 之间全为合数,那么小于 $n!$ 的所有素数全小于 n

记这些素数从小到大排列为 $p_1, p_2, \cdots, p_k$, 置

$$P = p_1 p_2 \cdots p_k + 1$$

因为 $2 = p_1 < p_2 < p_3 \cdots < p_k \leq n$, 故 $P < n!$
而 P 的素因子一定不在 $p_1, p_2, \cdots, p_k$中, 又 $P < n!$, 故 P 的素因子一定在 n 和 $n!$ 之间
矛盾! 故 n 和 $n!$ 之间必有素数
记 $f(n) = n!$, $f^{k+1}(n) = f\left(f^k(n)\right)$, 那么区间 $\left(f^k(3), f^{k+1}(3)\right)$ 中至少存在一个素数
且 $\bigcap\limits_{k\geq 1} \left(f^k(3), f^{k+1}(3)\right) = \varnothing$, 从而构成了 $\mathbb{N} \to \mathbb{P}$ 的一个单射, 所以 $|\mathbb{P}| \geq |\mathbb{N}| = +\infty$

1.2 最大公因子与最小公倍数

1. 设 n 是正整数, 证明: $\dfrac{21n+4}{14n+3}$ 是既约分数.

解答.
因为

$$(21n+4, 14n+3) = (7n+1, 14n+3) = (7n+1, 1) = 1$$

故 $\dfrac{21n+4}{14n+3}$ 是既约分数

2. 设 m, n 为正整数, m 为奇数, 证明:

$$(2^m - 1, 2^n + 1) = 1.$$

解答.
法一:
注意到

$$\begin{aligned}
(2^m - 1, 2^n + 1)(2^m - 1, 2^n - 1) &= (2^m - 1, (2^n + 1)(2^n - 1)) \\
&= \left(2^m - 1, 2^{2n} - 1\right) \\
&= 2^{(m,2n)} - 1 \\
&= 2^{(m,n)} - 1 \\
&= (2^m - 1, 2^n - 1)
\end{aligned}$$

因此 $(2^m-1,2^n+1)=1$

法二:

设 $d=(2^m-1,2^n+1)$, 那么

$$1\equiv(2^m)^n\equiv(2^n)^m\equiv(-1)^m\equiv-1\pmod d$$

这说明 $d=1$或2, 但 2^m-1, 2^n+1均为奇数, 于是 $d=1$

3. 设 m, n, a 均为正整数, $a\geq 2$, 证明:

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

解答.

不妨设 $m>n$, 对 m, n 辗转相除得

$$\begin{cases} m=q_0n+r_0,0\leq r_0<n\\ n=q_1r_0+r_1,0\leq r_1<r_0\\ \vdots\\ r_{k-1}=q_kr_{k-2}+r_k,r_k=0\end{cases}$$

于是对于 a^m-1 和 a^n-1 辗转相除也有

$$\begin{cases} a^m-1=a^{qn+r}-1=\sum\limits_{k=0}^{q-1}a^{kn+r}\cdot(a^n-1)+(a^r-1),0\leq a^r-1<a^n-1\\ \vdots\\ a^{r_{k-1}}-1=\sum\limits_{k=0}^{q_k-1}a^{kr_{k-2}+r_k}\cdot(a^{r_{k-2}}-1)+(a^{r_k}-1),a^{r_k}-1=0\end{cases}$$

故 $(a^m-1,a^n-1)=a^{r_{k-2}}-1=a^{(m,n)}-1$

4. 设 a, b, $c\in\mathbb{Z}$, $a\neq 0$. 则 $a\mid bc$ 当且仅当$\dfrac{a}{(a,b)}\mid c$.

解答.

记 $d=(a,b)$, 只需要注意到

$$\left(\frac{a}{d},\frac{b}{d}\right)=1,\quad (a,b)\mid b,\quad (a,b)\mid a$$

那么

$$a\mid bc\Leftrightarrow\frac{a}{d}\mid\frac{b}{d}c\Leftrightarrow\frac{a}{d}\mid c$$

5. m 和 n 是互素的正整数. 证明:

(1)对每个整数 a, $(a,mn)=(a,m)(a,n)$;

(2) mn 的每个正因子 d 均可惟一地表示成 $d=d_1d_2$, 其中 d_1 和 d_2 分别为 m 和 n 的正因子.

解答.

(1)设 $d_1=(a,m)$, $d_2=(a,n)$

$(a,mn)=d_1\left(\frac{a}{d_1},\frac{m}{d_1}n\right)=d_1\left(\frac{a}{d_1},n\right)=d_1d_2\left(\frac{a}{d_1d_2},\frac{n}{d_2}\right)=d_1d_2\left(\frac{a}{d_1d_2},1\right)=d_1d_2=(a,m)(a,n)$

(2) d 的素因子 p 必定整除 m, n其中一个, 否则与 $p\mid d$, $d\mid mn$矛盾, 则可以把 d 的素因子按两类划分, $A=\{p\in\mathbb{P}:p\mid d,p\mid m\}$, $B=\{p\in\mathbb{P}:p\mid d,p\mid n\}$ 满足 $A\cap B=\varnothing$, $A\cup B=\{p:p\mid d\}$ 那么 $d_1=\prod\limits_{p\in A}p^{r_p}$, $d_2=\prod\limits_{p\in B}p^{r_p}$, 其中 r_p 是素数 p 在 d 中的次数, 由于 m, n互素, 故 p 仅能整除 m, n其中一个, 这说明上述划分是唯一的, 进而说明 d_1, d_2 是唯一的

6. 设 n 为正整数, a, b 是不全为 0 的整数. 证明:

(1) $(a^n,b^n)=(a,b)^n$;

(2)若 a 和 b 是互素的正整数, $ab=c^n$, $c\in\mathbb{Z}$, 则 a 和 b 都是正整数的 n 次方幂. 事实上, $a=(a,c)^n$, $b=(b,c)^n$.

解答.

(1)令 $d=(a,b)$, 那么

$$(a^n,b^n)=d^n\left(\left(\frac{a}{d}\right)^n,\left(\frac{b}{d}\right)^n\right)=d^n=(a,b)^n$$

(2)

$$(a,c)^n=(a^n,c^n)=(a^n,ab)=a$$

同理 $(b,c)^n=b$

7. 设 a, b 均是绝对值大于或等于 2 的整数, 且两者绝对值不同时为 2. 证明方程 $ax+by=(a,b)$ 有整数解 (x,y) 满足 $0<|x|<b$, $0<|y|<a$.

解答.

设 $ax+by=(a,b)$有解(x_0,y_0), 那么其全部解为 $\begin{cases}x=x_0+\dfrac{b}{(a,b)}n\\ y=y_0-\dfrac{a}{(a,b)}n\end{cases}$, $n\in\mathbb{Z}$

1° 若 $\frac{b}{(a,b)}\mid x_0$, 则存在 n_0 使得 $x_0+\frac{b}{(a,b)}n_0=0\Rightarrow b\mid(a,b)\Rightarrow(a,b)=b$,

那么可以取 $\begin{cases} x_0 = 0 \\ y_0 = 1 \end{cases}$, 又 $(a,b) = b \geq 2$, 再令 $n = -1$ 有 $0 < \left|-\dfrac{b}{(a,b)}\right| < b$, $0 < \left|1 + \dfrac{a}{(a,b)}\right| < a$

2° 若 $\dfrac{b}{(a,b)} \nmid x_0$, 那么存在 n_0 使得 $0 < \left|x_0 + \dfrac{b}{(a,b)}n_0\right| < b$, 故

$$\begin{aligned} 0 \leq \left|y_0 - \frac{a}{(a,b)}n_0\right| &= \left|\frac{(a,b) - ax_0}{b} - \frac{a}{(a,b)}n_0\right| \\ &= \left|\frac{(a,b) - a\left(x_0 + \dfrac{b}{(a,b)}n_0\right)}{b}\right| \\ &\leq \left|\frac{(a,b) + a\,(b-1)}{b}\right| \\ &\leq a \end{aligned}$$

若两处不等号可取等, 那么由 1° 类似可知 $(a,b) = a$, 也可构造一组符合要求的解

题目7的注记.

[1] 原题没有"且两者绝对值不同时为 2"这一条件, 没有这一条件原题是错误的, 例如方程 $2x + 2y = 2$ 就没有符合条件的解.

8. 设 a 和 b 是互素的正整数, 证明:当 $n > ab - a - b$ 时, 方程 $ax + by = n$ 有非负整数解, 而方程 $ax + by = ab - a - b$ 没有非负整数解.

解答.

因为 $(a,b) = 1$, 故 $ax + by = n$ 必有整数解 (x_0, y_0), 进而全部解为 $\begin{cases} x = x_0 - bt \\ y = y_0 + at \end{cases}$

由抽屉原理不难知道总存在 t_0 使得 $0 \leq x_0 - bt_0 < b$

进而 $y_0 + at_0 = \dfrac{n - ax_0}{b} + at_0 = \dfrac{n - a\,(x_0 - bt_0)}{b} \geq \dfrac{n - a(b-1)}{b} \geq 0$

注意到 $a\,(b-1) + b\,(-1) = ab - a - b$, 进而 $ax + by = ab - a - b$ 的所有解为 $\begin{cases} x = b - 1 - bt \\ y = -1 + at \end{cases}$

而不等式组 $\begin{cases} x = b - 1 - bt \geq 0 \\ y = -1 + at \geq 0 \end{cases}$ 是无解的, 即方程 $ax + by = ab - a - b$ 没有非负整数解

9. 用辗转相除法求 963 和 657 的最大公因子, 并求出方程 $963x + 657y = (963, 657)$的全部整数解.

解答.

辗转相除如下

$$
\begin{aligned}
963 &= 657 \times 1 + 306 \\
657 &= 306 \times 2 + 45 \\
306 &= 45 \times 6 + 36 \\
45 &= 36 \times 1 + 9 \\
36 &= 4 \times 9
\end{aligned}
$$

故 $(963, 657) = 9$, 再带回可知方程的全部解为$\begin{cases} x = 73n + 58 \\ y = -107n - 85 \end{cases}$, $n \in \mathbb{Z}$

10. 求下列方程组的全部整数解:

(1) $6x + 20y - 15z = 23$;

(2) $25x + 13y + 7z = 2$.

解答.

(1) $\begin{cases} x = 5n_1 + 3 \\ y = 3n_2 + 1 \\ z = 2n_1 + 4n_2 + 1 \end{cases}$, $n_1, n_2 \in \mathbb{Z}$

(2) $\begin{cases} x = n_1 \\ y = 4n_1 + 7n_2 + 5 \\ z = -11n_1 - 13n_2 - 9 \end{cases}$, $n_1, n_2 \in \mathbb{Z}$

11. 设 n 为正整数, k 为正奇数. 证明:

$$(1 + 2 + \cdots + n) \mid \left(1^k + 2^k + \cdots + n^k\right).$$

解答.

即证

$$n(n+1) \mid 2\left(1^k + 2^k + \cdots + n^k\right)$$

因为

$$2\left(1^k + 2^k + \cdots + n^k\right) = \sum_{i=0}^{n} i^k + (n+1-i)^k \equiv \sum_{i=0}^{n} i^k + (-k)^k \equiv 0 \pmod{n+1}$$

所以 $n+1 \mid 2\left(1^k+2^k+\cdots+n^k\right)$

因为

$$2\left(1^k+2^k+\cdots+n^k\right)=2n^k+\sum_{i=1}^{n-1} i^k+(n-i)^k \equiv 0 \pmod n$$

所以 $n \mid 2\left(1^k+2^k+\cdots+n^k\right)$

又 $(n,n+1)=1$, 故 $n(n+1) \mid 2\left(1^k+2^k+\cdots+n^k\right)$

12. 设 $f(x)=x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n$ 是首项系数为 1 的整系数多项式(即 $a_i \in \mathbb{Z}$, $1 \le i \le n$), 则 $f(x)$ 的每个有理数根必为整数.

解答.

设 $f(x)$ 的有理根为 $\dfrac{p}{q}$, $(p,q)=1$

$$f\left(\frac{p}{q}\right)=0 \Rightarrow \left(\frac{p}{q}\right)^n+a_1\left(\frac{p}{q}\right)^{n-1}+\cdots+a_n=0 \Rightarrow p^n+a_1p^{n-1}q+\cdots+a_nq^n=0$$

因为 $q \mid 0$, 那么

$$q \mid p^n+a_1p^{n-1}q+\cdots+a_nq^n \Rightarrow q \mid p^n \Rightarrow q \mid p \Rightarrow \frac{p}{q} \in \mathbb{Z}$$

13. 设 m 和 n 为正整数, 则在 $n, 2n, \cdots, mn$ 这 m 个数中恰有 (m,n) 个是 m 的倍数.

解答.

设 $d=(m,n)$, 那么 $m \mid kn \Leftrightarrow \dfrac{m}{d} \mid k\dfrac{n}{d} \Leftrightarrow \dfrac{m}{d} \mid k$, $1 \le k \le m$

进而符合条件的 k 有 $\left[\dfrac{m}{\frac{m}{d}}\right]=[d]=d=(m,n)$个

14. (1)若 m 为正整数, 证明: 若 2^m+1 为素数, 则 m 为 2 的方幂.

(2)对 $n \ge 0$, 记 $F_n=2^{2^n}+1$. 证明: 当 $m>n\ge 0$ 时, $(F_m,F_n)=1$. 由此证明素数有无限多个.

解答.

(1)设 $m=2^rq$, q是奇数, 那么

$$2^m+1=2^{rq}+1=(2^r)^q+1=(2^r+1)\left(2^{r(q-1)}-2^{r(q-2)}+\cdots-2^r+1\right)$$

若 $q \ge 3$, 那么 2^m+1 存在非平凡因子, 不为素数

故 $q=1$, 即 m 为 2 的方幂

(2)注意到

$$F_m-2=2^{2^n}-1=\left(2^{2^{m-1}}+1\right)\left(2^{2^{m-1}}-1\right)=\cdots=\prod_{k=1}^{m-1}F_k\left(2^{2^0}-1\right)=\prod_{k=1}^{m-1}F_k$$

设 $d=(F_m,F_n)$, 由上式知 $d\mid F_m-2\Rightarrow d\mid -2$, 进而 $d=1$或 2
而 F_m, F_n为奇数, 没有偶因子, 故 $d=1$

15. (1)设 m, n 都是大于 1 的整数. 证明:若 m^n-1 是素数, 则 $m=2$ 并且 n 是素数.
(2)对于每个素数 p, 记 $M_p=2^p-1$.证明:若 p 和 q 是不同的素数, 则 $(M_p,M_q)=1$.

解答.
(1)因为
$$m^n-1=(m-1)\left(1+m+\cdots+m^{n-1}\right)$$
若 $m>2$, 那么 m^n-1 有因子 $m-1$, 故 $m=2$ 若 n 不是素数, 设 $n=st$, 那么
$$2^{st}-1=(2^s-1)\sum_{k=0}^{t-1}2^k$$
故 n 必为素数
(2)
$$(M_p,M_q)=(2^p-1,2^q-1)=2^{(p,q)}-1=1$$

16. 设 m 和 n 是互素的非零整数. 证明: 对每个整数 a, 如果 $m\mid a$, $n\mid a$, 则 $mn\mid a$.

解答.
设 $a=md_1=nd_2$, 那么 $n\mid md_1$, 又 $(m,n)=1$, 故 $n\mid d_1$
进而 $mn\mid md_1$, 即 $mn\mid a$

1.3 惟一分解定理

1. 用惟一分解定理和推论 1.3.2 证明引理 1.2.4 和引理 1.2.6 的诸命题.

解答.
只证明 **引理 1.2.4 (6)**, **引理 1.2.6 (4)(5)**

引理 1.2.4 (6) 若 c 为非零整数, a, $b\in\mathbb{Z}$, $c\mid ab$, $(c,b)=1$, 则 $c\mid a$. 特别地, 若 p 为素数, $p\mid ab$, 则 $p\mid a$ 或 $p\mid b$.

证明. 设 a, b, c 的标准分解为 $\prod_{k=1}^{n}p_k^{\alpha_k}$, $\prod_{k=1}^{n}p_k^{\beta_k}$, $\prod_{k=1}^{n}p_k^{\gamma_k}$
只需证明在 $\min\{\beta_k,\gamma_k\}=0$ 且 $\gamma_k\le\alpha_k+\beta_k$ 的情况下有 $\gamma_k\le\alpha_k$
1° 若 $\min\{\beta_k,\gamma_k\}=\beta_k=0$, 那么根据 $\gamma_k\le\alpha_k+\beta_k$ 有 $\gamma_k\le\alpha_k$
2° 若 $\min\{\beta_k,\gamma_k\}=\gamma_k=0$, 那么 $\alpha_k\ge 0=\gamma_k$ □

引理 1.2.6 (4) $(a,b)\,[a,b]=|ab|$.

证明. 设 a, b 的标准分解为 $\prod\limits_{k=1}^{n}p_k^{\alpha_k}$, $\prod\limits_{k=1}^{n}p_k^{\beta_k}$
所要证的即为

$$\min\{\alpha_k,\beta_k\}+\max\{\alpha_k,\beta_k\}=\alpha_k+\beta_k$$

这是显然的 □

引理 1.2.6 (5) 若 $a_1,\cdots,a_n$ 两两互素, 则 $[a_1,\cdots,a_n]=|a_1\cdots a_n|$.

证明. 设 a_i 的标准分解为 $\prod\limits_{k=1}^{n}p_k^{\alpha_k^{(i)}}$, 那么 $\forall i,j$, 有 $\min\left\{\alpha_k^{(i)},\alpha_k^{(j)}\right\}=0$
所以

$$\alpha_k^{(1)}+\cdots+\alpha_k^{(n)}=\max\left\{\alpha_k^{(1)},\cdots,\alpha_k^{(n)}\right\}$$

这就是所要证的 □

2. 用惟一分解定理证明习题 1.2 的第 5 题, 第 6 题和第 16 题.

解答.

1.2.5 m 和 n 是互素的正整数. 证明:
(1) 对每个整数 a, $(a,mn)=(a,m)\,(a,n)$;
(2) mn 的每个正因子 d 均可惟一地表示成 $d=d_1d_2$, 其中 d_1 和 d_2 分别为 m 和 n 的正因子.

证明. (1) 设 a, m, n 的标准分解为 $\prod\limits_{k=1}^{n}p_k^{\alpha_k}$, $\prod\limits_{k=1}^{n}p_k^{\beta_k}$, $\prod\limits_{k=1}^{n}p_k^{\gamma_k}$
则只需证明在 $\min\{\beta_k,\gamma_k\}=0$ 的情况下有

$$\min\{\alpha_k,\beta_k+\gamma_k\}=\min\{\alpha_k,\beta_k\}+\min\{\alpha_k,\gamma_k\}$$

由 β_k, γ_k 的对称性, 不妨设 $\min\{\beta_k,\gamma_k\}=\beta_k=0$, 进而结论是显然的
(2) 由惟一分解定理可知, d 的相同的素因子只能来自 β_k, γ_k 的其中一个, 故这种分解是惟一的 □

1.2.6 设 n 为正整数, a, b 是不全为 0 的整数. 证明:
(1) $(a^n,b^n)=(a,b)^n$;
(2) 若 a 和 b 是互素的正整数, $ab=c^n$, $c\in\mathbb{Z}$, 则 a 和 b 都是正整数的 n 次方幂. 事实上, $a=(a,c)^n$, $b=(b,c)^n$.

证明. (1) 设 a, b 的标准分解为 $\prod\limits_{k=1}^{n} p_k^{\alpha_k}$, $\prod\limits_{k=1}^{n} p_k^{\beta_k}$

只需证明

$$\min\left\{\alpha_k^n, \beta_k^n\right\} = \min\left\{\alpha_k, \beta_k\right\}^n$$

这是显然的

(2) 因为 c 的素因子只能来自 a, b 中的其中一个, 所以 a, b 中每个素因子的次数都是 n 的倍数, 即 a, b 是 n 次方幂

进而 $(a,c)^n = (a^n, c^n) = a$, 同理 $(b,c)^n = b$ □

1.2.16 设 m 和 n 是互素的非零整数. 证明: 对每个整数 a, 如果 $m \mid a$, $n \mid a$, 则 $mn \mid a$.

证明. 设 a, b, c 的标准分解为 $\prod\limits_{k=1}^{n} p_k^{\alpha_k}$, $\prod\limits_{k=1}^{n} p_k^{\beta_k}$, $\prod\limits_{k=1}^{n} p_k^{\gamma_k}$

只需证明当$\min\left\{\alpha_k, \beta_k\right\} = 0$ 且 α_k, $\beta_k \leq \gamma_k$ 时有

$$\alpha_k + \beta_k \leq \gamma_k$$

这是显然的 □

3. 设a, b, c均为正整数, 证明:

(1) $(a, [b,c]) = [(a,b), (a,c)]$;

(2) $[a, (b,c)] = ([a,b], [a,c])$.

解答.

设a, b, c 的标准分解为 $a = \prod\limits_{i=1}^{n} p_i^{r_i}$, $b = \prod\limits_{i=1}^{n} p_i^{s_i}$, $c = \prod\limits_{i=1}^{n} p_i^{t_i}$

(1) 只需验证 $\min\left\{r_i, \max\left\{s_i, t_i\right\}\right\} = \max\left\{\min\left\{r_i, s_i\right\}, \min\left\{r_i, t_i\right\}\right\}$

注意到 s_i, t_i 对称, 所以只用考虑 $r_i \geq s_i \geq t_i$, $s_i \geq r_i \geq t_i$, $s_i \geq t_i \geq r_i$三种情况即可

依次验证是容易的

(2) 只需验证 $\max\left\{r_i, \min\left\{s_i, t_i\right\}\right\} = \min\left\{\max\left\{r_i, s_i\right\}, \max\left\{r_i, t_i\right\}\right\}$

注意到 s_i, t_i 对称, 所以只用考虑 $r_i \geq s_i \geq t_i$, $s_i \geq r_i \geq t_i$, $s_i \geq t_i \geq r_i$ 三种情况即可

依次验证是容易的

4. 正整数 n 叫做无平方因子, 是指不存在整数 $m \geq 2$, 使得 $m^2 \mid n$. 证明:

(1) 正整数 n 是无平方因子的当且仅当 $n = 1$ 或者是不同素数因子的乘积.

(2) 每个正整数 n 均可惟一地表示成 $n = m^2 \cdot n'$, 其中 m^2 是正整数 m 的平方(叫做平方数), 而 n' 是无平方因子整数.

解答.

(1) 必要性是显然的, 下证充分性

设正整数 n 的标准分解为 $\prod_{k=1}^{n} p_k^{\alpha_k}$

若存在$\alpha_k \geq 2$, 那么 n 有平方因子 p_k^2, 故 $a_k \leq 1$, $k = 1, 2, \cdots, n$

当 $a_k = 0$, $k = 1$, 2, $\cdots$, n 时, 即 $n = 1$; 当存在 $a_k \neq 0$ 时, 即 n 为不同素因子的乘积

(2) 设正整数 n 的标准分解为 $\prod_{k=1}^{n} p_k^{\alpha_k}$

考虑 α_k 与 2 的带余除法 $\alpha_k = 2 \times q_k + r_k$, $0 \leq r_k \leq 1$

那么

$$n = \prod_{k=1}^{n} p_k^{\alpha_k} = \prod_{k=1}^{n} p_k^{2q_k} \cdot \prod_{k=1}^{n} p_k^{r_k}$$

其中 $\prod_{k=1}^{n} p_k^{2q_k}$ 是一个平方数; 而根据 (1), $\prod_{k=1}^{n} p_k^{r_k}$ 是一个无平方因子整数

1.4 数论函数、莫比乌斯反演公式

1. 以 $\omega(n)$ 表示不同正整数 n 的不同素因子的个数, 即 $\omega(1) = 0$, 而当 $n \geq 2$, $n = p_1^{a_1} \cdots p_r^{a_r}$(标准分解式)时, $\omega(n) = r$. 证明:

(1) $\sum_{d:d|n} |\mu(d)| = 2^{\omega(n)}$;

(2) $\sum_{d:d|n} \mu(d)\tau(d) = (-1)^{\omega(n)}$;

(3) $\sum_{d:d|n} \mu(d)\sigma(d) = (-1)^{\omega(n)} \prod_{p|n} p$, 这里乘积 $\prod_{p|n}$ 表示 p 过 n 的不同素因子.

解答.

(1) n 的因子 $d = \prod_{k=1}^{r} p_k^{\beta_k}$, $\beta_k \leq \alpha_k$

$|\mu(d)| = 1$ 当且仅当 $\beta_k = 0, 1$; 故共有 $2^r = 2^{\omega(n)}$ 个因子 d 使得 $|\mu(d)| = 1$, 即 $\sum_{d:d|n} |\mu(d)| = 2^{\omega(n)}$

(2) 只需考虑 $\mu(d) \neq 0$ 的情况, 此时 d 的素因子的幂次均为 1, 设 d 含有 s $(0 \leq s \leq \omega(n))$ 个素因子

那么 $\mu(d) = (-1)^s$, $\tau(d) = 2^s$, 故

$$\sum_{d|n} \mu(d)\tau(d) = \sum_{s=0}^{\omega(n)} \binom{s}{\omega(n)} (-1)^s 2^s = \sum_{s=0}^{\omega(n)} (-2)^s \cdot 1^{\omega(n)-s} = ((-2) + 1)^{\omega(n)} = (-1)^{\omega(n)}$$

(3) 只需考虑 $\mu(d) \neq 0$ 的情况, 此时 d 的素因子的幂次均为 1, 设 d 含有 s $(0 \leq s \leq \omega(n))$ 个素因子

那么

$$\sum_{d|n}\mu(d)\sigma(d)=\sum_{s=0}^{\omega(n)}(-1)^s\sum_{p_1<\cdots<p_s}\sigma(p_1)\cdots\sigma(p_s)=\prod_{p|n}(1-\sigma(p))=\prod_{p|n}-p=(-1)^{\omega(n)}\prod_{p|n}p$$

题目1的注记.

[1] 也可用莫比乌斯反演, 例如 (3), 只需证明

$$\mu(n)\sigma(n)=\sum_{d|n}\mu\left(\frac{n}{d}\right)(-1)^{\omega(d)}\prod_{p|d}p$$

而

$$\sum_{d|n}\mu\left(\frac{n}{d}\right)(-1)^{\omega(d)}\prod_{d'|d}d'=\sum_{d|n}\mu(n)\prod_{p|d}p=\mu(n)\sum_{d|n}\prod_{p|d}p=\mu(n)\sigma(n)$$

所以根据莫比乌斯反演结论成立.

[2] 称

$$\sigma_k=\sum_{1\le i_1<\cdots<i_k\le n}x_{i_1}\cdots x_{i_k}$$

为 k 次基本对称多项式, 它有如下的性质

$$\prod_{k=1}^{n}(x-x_k)=\sum_{k=0}^{n}(-1)^k\sigma_k x^{n-k}$$

因此

$$\sum_{s=0}^{\omega(n)}(-1)^s\sum_{d_1<\cdots<d_s}\sigma(d_1)\cdots\sigma(d_s)=\prod_{p|n}(1-\sigma(p)).$$

[3] 也可采用积性数论函数的性质. 以 (2) 举例, 不难验证 $\mu(n)$, $\tau(n)$ 是积性数论函数, 那么

$$(\mu\cdot\tau)*\{1\}(n)=\sum_{d|n}\mu(d)\tau(d)$$

也是积性数论函数. 设 n 的标准分解为 $\prod_{i=1}^{k}p_i^{\alpha_i}$ (这意味着 $\omega(n)=k$), 那么

$$\sum_{d|n}\mu(d)\tau(d)=\prod_{i=1}^{k}\sum_{d|p_i^{\alpha_i}}\mu(d)\tau(d)=\prod_{i=1}^{k}-1=(-1)^{\omega(n)}.$$

2. 如果 f 是积性数论函数, 证明:

$$\sum_{d:d|n}\mu(d)f(d)=\prod_{p|n}(1-f(p)).$$

解答.

只需考虑 n 的素因子幂次全为 1 时的情况

法一(齐次对称多项式):

$$\sum_{d|n}\mu(d)f(d)=\sum_{s=0}^{\omega(n)}(-1)^s\sum_{p_1<\cdots<p_n}f(p_1\cdots p_2)=\sum_{s=0}^{\omega(n)}(-1)^s\sum_{p_1<\cdots<p_n}f(p_1)\cdots f(p_n)=\prod_{p|n}(1-f(p))$$

法二(莫比乌斯反演):

记 $g(n)=\prod\limits_{p|n}(1-f(p))$

$$\sum_{d|n}\mu\left(\frac{n}{d}\right)g(d)=\sum_{d|n}(-1)^{\omega(n)-\omega(d)}\prod_{p|d}(1-f(p))=(-1)^{\omega(n)}\sum_{d|n}(-1)^{\omega(d)}\prod_{p|d}(1-f(p))=\mu(n)f(n)$$

故由莫比乌斯反演知结论成立

题目2的注记.

[1] 此处的 $\omega(n)$ 与 1 题含义相同;

[2] 1(3) 可以看作本题的一个特殊情况.

3. 设 f 是数论函数. 证明: f 对于卷积有逆 (即存在数论函数 g, 使得 $f*g=e$) 当且仅当 $f(1)\neq 0$.

解答.

先证明必要性

只需注意到

$$f*g(1)=f(1)g(1)=1\Rightarrow f(1)\neq 0$$

再证明充分性

下面递归地定义 g 使得 $f*g=e$

1. 由 $f*g(1)=f(1)g(1)=1$ 且 $f(1)\neq 0$ 知 $g(1)=\dfrac{1}{f(1)}$
2. 假设 $\forall i=2,3,\cdots,n$, $g(i)$ 已被良好地定义, 那么根据

$$f*g(n+1)=\sum_{d|n+1}f(d)g\left(\frac{n+1}{d}\right)=0$$

可得

$$g(n+1)=-\frac{\sum\limits_{\substack{d|n+1\\d\neq 1}}f(d)g\left(\dfrac{n+1}{d}\right)}{f(1)}$$

因而可以良好的定义 $g(n)$, $n \in \mathbb{N}_+$

4. 证明: 数论函数的卷积运算 $*$ 满足结合律, 即对任意数论函数 f, g 和 h, $(f*g)*h = g*(f*h)$.

解答.

根据卷积的定义有

$$\begin{aligned} ((f*g)*h)(n) &= \sum_{xy=n} (f*g)(x)h(y) \\ &= \sum_{xy=n} \left(\sum_{zw=x} f(z)g(w) \right) h(y) \\ &= \sum_{xy=n} \sum_{zw=x} f(z)g(w)h(y) \\ &= \sum_{xyz=n} f(x)g(y)h(z) \end{aligned}$$

类似的也可以得到

$$(g*(f*h))(n) = \sum_{xyz=n} f(x)g(y)h(z)$$

故卷积满足结合律

5. 满足 $\sigma(n) = 2n$ 的正整数 n 叫做完全数. 由于 $\sigma(n) - n$ 是 n 的全部小于 n 的正因子之和, 所以 n 是完全数当且仅当 n 等于它的所有正因子 (n 除外) 之和.

(1) 验证 6, 28 是完全数;

(2) 证明欧拉的结果, 正偶数 n 是完全数, 当且仅当 $n = 2^{a-1}(2^a - 1)$, 其中 $a \geq 2$, 而 $2^a - 1$ 是素数.

解答.

(1) 6 的正因子有 1, 2, 3, 6, $1+2+3+6 = 2 \times 6$, 故 6 是完全数

28 的正因子有 1, 2, 4, 7, 14, 28, $1+2+4+7+14+28 = 2 \times 28$, 故 28 是完全数

(2) 充分性是显然的, 下只证必要性

设偶数 $n = 2^{a-1}q$, 其中 q 是奇数, 那么 $\sigma(n) = \sigma(2^{a-1})\sigma(q) = (2^a - 1)\sigma(q) = 2^a q$

于是 $2^a - 1 \mid q$, 设 $q = (2^a - 1)l$, 那么

$$\sigma(q) = \frac{2^a q}{2^a - 1} = 2^a l$$

而 q 的两个因子 $(2^a - 1)l$, l 的和已为 $2^a l$, 故 $l = 1$

这说明 $\sigma(2^a - 1) = \sigma(2^a)$, 故 $2^a - 1$ 为素数

6. 证明: 对每个正整数 n,

$$\sum_{d|n}\tau(d)\mu\left(\frac{n}{d}\right)=1,\sum_{d|n}\sigma(d)\mu(\frac{n}{d})=n.$$

解答.

注意到 τ, μ 都是积性数论函数, 那么 $\tau*\mu$ 也是积性数论函数, 设 n 的标准分解为 $\prod\limits_{i=1}^{k}p_i^{\alpha_i}$, 那么

$$\sum_{d|n}\tau(d)\mu\left(\frac{n}{d}\right)=\prod_{i=1}^{k}\sum_{d|p_i^{\alpha_i}}\tau(d)\mu\left(\frac{n}{d}\right)=\prod_{i=1}^{k}\left(\tau(n)-\tau\left(p_i^{\alpha_i-1}\right)\right)=\prod_{i=1}^{k}1=1$$

类似地

$$\sum_{d|n}\sigma(d)\mu\left(\frac{n}{d}\right)=\prod_{i=1}^{k}\sum_{d|p_i^{\alpha_i}}\sigma(d)\mu\left(\frac{n}{d}\right)=\prod_{i=1}^{k}\left(\sigma(n)-\sigma\left(p_i^{\alpha_i-1}\right)\right)=\prod_{i=1}^{k}p_i^{\alpha_i}=n$$

2 同余

2.1 同余式和同余类

1. 设 m 为正整数, $(a,m)=1$. 我们用 a^{-1} 表示同余方程 $ax\equiv 1 \pmod m$ 的任何一个整数解 (即 $a^{-1}\in\mathbb{Z}$, $aa^{-1}\equiv 1 \pmod m$).证明:

(1) 若 $(a,m)=(b,m)=1$, 则 $a\equiv b \pmod m$ 当且仅当 $a^{-1}\equiv b^{-1} \pmod m$;

(2) 若 $\left\{r_1,r_2,\cdots,r_{\varphi(m)}\right\}$ 是模 m 的缩系, 则 $\left\{r_1^{-1},r_2^{-1},\cdots,r_{\varphi(m)}^{-1}\right\}$ 也是模 m 的缩系.

解答.

(1) 必要性: 两边同乘 $a^{-1}b^{-1}$ 即得 $a^{-1}\equiv b^{-1} \pmod m$

充分性: 两边同乘 ab 即得 $a\equiv b \pmod m$

(2) 设 $d=(r_i^{-1},m)$, 那么 $\dfrac{r_ir_i^{-1}-1}{m}\in\mathbb{Z}$, 设 $z=\dfrac{r_ir_i^{-1}-1}{m}$

那么 $r_ir_i^{-1}-mz=1$, 这说明关于 x, y 的方程 $r_i^{-1}x-my=1$ 有解, 故 $d\mid 1$, 即 $d=1$

而 $r_i^{-1}\equiv r_j^{-1} \pmod m\Leftrightarrow r_i\equiv r_j \pmod m$, 所以 $\left\{r_1^{-1},r_2^{-1},\cdots,r_{\varphi(m)}^{-1}\right\}$ 也是模 m 的缩系

2. 设正整数的 n 的十进制表示为

$$n=a_0+a_1\cdot 10+a_2\cdot 10^2+\cdots+a_k\cdot 10^k,$$

证明:

$$n \equiv \begin{cases} a_0 + a_1 + \cdots + a_k \pmod 9 \\ a_0 - a_1 + a_2 - \cdots + (-1)^k a_k \pmod{11} \end{cases}.$$

用这些结果来计算 12345×6789 被 9 和被 11 除所得的余数.

解答.

只需注意到 $10^k \equiv 1^k \equiv 1 \pmod 9$, $10^k \equiv (-1)^k \pmod{11}$, 那么结论是显然的

所以

$$12345 \times 6789 \equiv 15 \times 30 \equiv 6 \times 3 \equiv 0 \pmod 9$$

$$12345 \times 6789 \equiv 3 \times (-2) \equiv 5 \pmod{11}$$

3. 解下列同余方程.

(1) $8x \equiv 5 \pmod 3$; (2) $60x \equiv 7 \pmod{37}$.

解答.

(1) $x \equiv 1 \pmod 3$

(2) $x \equiv 18 \pmod{37}$

4. 对每个正整数 n 证明:

(1) $n^2 \not\equiv 2 \pmod 3$; (2) $n^2 \equiv 0$ 或 $1 \pmod 4$; (3) $n^3 \equiv 0, 1$ 或 $-1 \pmod 9$;

(4) $n^4 \equiv 0$ 或 $1 \pmod{16}$.

解答.

(1) 注意到 $(3k)^2 \equiv 0 \pmod 3$, $(3k+1)^2 \equiv 1 \pmod 3$, $(3k+2)^2 \equiv 1 \pmod 3$

故 $n^2 \not\equiv 2 \pmod 3$

(2) 注意到 $(2k)^2 \equiv 0 \pmod 4$, $(2k+1)^2 \equiv 1 \pmod 4$

故 $n^2 \equiv 0$ 或 $1 \pmod 4$

(3) 注意到 $(3k)^3 \equiv 0 \pmod 9$, $(3k+1)^3 \equiv (6k+1)(3k+1) \equiv 1 \pmod 9$, $(3k+2)^3 \equiv (3k+4)(3k+2) \equiv -1 \pmod 9$

故 $n^3 \equiv 0, 1$ 或 $-1 \pmod 9$

(4) 注意到 $(2k)^4 \equiv 0 \pmod{16}$, $(2k+1)^4 \equiv 16k^4 + 32k^3 + 24k^2 + 8k + 1 \equiv 8k(k+1) + 1 \equiv 1 \pmod{16}$

故 $n^4 \equiv 0$ 或 $1 \pmod{16}$

5. 设 a 为奇数, $n \geq 1$. 证明: $a^{2^n} \equiv 1 \pmod{2^{n+2}}$.

解答.

注意到

$$a^{2^n}-1=\left(a^{2^{n-1}}+1\right)\left(a^{2^{n-1}}-1\right)=\left(a^{2^{n-1}}+1\right)\left(a^{2^{n-2}}+1\right)\left(a^{2^{n-2}}-1\right)=\cdots=\left(a^2-1\right)\prod_{k=1}^{n-1}\left(a^{2^k}+1\right)$$

因为 a 为奇数, 那么 $2 \mid a^{2^k}+1,\ k=1,\ 2,\ \cdots,\ n-1$

设 $a=2k+1$, 那么 $a^2-1=4k(k+1)$, k 和 $k+1$ 中必有一偶, 所以 $2 \mid k(k+1)$, 进而 $8 \mid a^2-1$

进而 $2^{n+2} \mid \left(a^2-1\right)\prod\limits_{k=1}^{n-1}\left(a^{2^k}+1\right)$, 即 $a^{2^n} \equiv 1 \pmod{2^{n+2}}$

6. (1) 证明: 当 $n \geq 3$ 时, $\varphi(n)$ 为偶数.

(2) 证明: 当 $n \geq 2$ 时, $\sum\limits_{\substack{i=1 \\ (i,n)=1}}^{n} i=\dfrac{1}{2}n\varphi(n)$.

解答.

(1) 由于 φ 是积性函数, 只需证明 $\varphi(p^\alpha)$ 是偶数即可, 而

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

显然为偶数

(2)注意到

$$2\sum_{\substack{i=1 \\ (i,n)=1}}^{n} i=\sum_{\substack{i=1 \\ (i,n)=1}}^{n} i+(n-i)=n\sum_{\substack{i=1 \\ (i,n)=1}}^{n} 1=n\varphi(n)$$

即

$$\sum_{\substack{i=1 \\ (i,n)=1}}^{n} i=\frac{1}{2}n\varphi(n)$$

7. 设 m 和 n 时正整数, $m=nt(t \in \mathbb{Z})$. 证明: 模 n 的每个同余类都是模 m 的 t 个同余类之并.

解答.

模 n 的同余类为 $A_i=\{kn+i : k \in \mathbb{Z}\}$, $i=0,\ 1,\ \cdots,\ n-1$

模 m 的同余类为 $B_j=\{km+j : k \in \mathbb{Z}\}$, $j=0,\ 1,\ \cdots,\ m-1$

因为 $m=nt$, 因此 $B_{i+kn}=\{(kt+k)n+i : k \in \mathbb{Z}\} \subset A_i$

故 $A_i=B_i \cap B_{i+n} \cap \cdots \cap B_{i+(t-1)n}$

8. 对每个 $n \geq 1$, 证明:

(1) $\sum_{d|n} \varphi(d) = n$; (2) $\sum_{d|n} \frac{\mu(d)}{d} = \frac{\varphi(n)}{n}$.

解答.

(1) 因为 φ 是积性函数, 那么 $(\varphi * 1)(n) = \sum_{d|n} \varphi(d)$ 也是积性函数, 进而只需证明 n 为素数幂的情况

$$\sum_{d|p^\alpha} \varphi(d) = \varphi(1) + \sum_{i=1}^{\alpha} p^i - p^{i-1} = p^\alpha$$

(2)等式左右两端均为积性函数, 那么只用验证素数幂时的情况

$$\sum_{d|p^\alpha} \frac{\mu(d)}{d} = \sum_{k=0}^{\alpha} \frac{\mu\left(p^k\right)}{p^k} = 1 - \frac{1}{p}$$

而

$$\frac{\varphi\left(p^\alpha\right)}{p^\alpha} = \frac{p^\alpha - p^{\alpha-1}}{p^\alpha} = 1 - \frac{1}{p}$$

故所证等式成立

9. 设 a, b 是互素的整数, $a + b \neq 0$, p 为奇素数.

证明: $\left(a+b, \frac{a^p + b^p}{a+b}\right) = 1$ 或 p, 并且说明这两种情形都会出现.

解答.

注意到

$$\begin{aligned}\frac{a^p + b^p}{a+b} \equiv & a^{p-1} - a^{p-2}b + \cdots + b^{p-1} \\ \equiv & pa^{p-1} \pmod{a+b}\end{aligned}$$

同理

$$\frac{a^p + b^p}{a+b} \equiv pb^{p-1} \pmod{a+b}$$

那么 $d \mid pa^{p-1}$ 且 $d \mid pb^{p-1}$, 而 $(a,b)=1$, 故 $d \mid p$, 进而 $d = 1, p$

取 $a = 2$, $b = 3$, 当 $p = 3$ 时, $\left(a+b, \frac{a^p + b^p}{a+b}\right) = 1$; $p = 5$ 时, $\left(a+b, \frac{a^p + b^p}{a+b}\right) = 5$

10. 设 $a, m \in \mathbb{Z}$, $m \geq 2$, $(a, m) = 1$. 计算 $\sum_{x=0}^{m-1} \left[\frac{ax}{m}\right]$.

解答.

引理 若 $x+y\in\mathbb{Z}$, 且 x, y 不为整数, 那么 $[x]+[y]=x+y-1$.

证明. 因为 x, y 不为整数, 所以 $[x]<x$, $[y]<y$,那么 $[x]+[y]<x+y$
而 $[x]+[y]$, $x+y\in\mathbb{Z}$, 由整数的离散性, 上式与 $[x]+[y]\le x+y-1$ 等价
另一方面, 熟知不等式 $[x]+[y]\ge[x+y]-1$, 与上式结合得

$$x+y-1\le[x]+[y]\le x+y-1$$

故 $[x]+[y]=x+y-1$ □

那么

$$\begin{aligned}\sum_{x=0}^{m-1}\left[\frac{ax}{m}\right]&=\frac{1}{2}\sum_{x=1}^{m-1}\left[\frac{ax}{m}\right]+\left[\frac{a(m-x)}{m}\right]\\&=\frac{1}{2}\sum_{x=1}^{m-1}\frac{ax+a\left(m-x\right)}{m}-1\\&=\frac{(a-1)(m-1)}{2}\end{aligned}$$

因为 $(a.m)=1$, 故 $\left[\dfrac{ax}{m}\right]$, $\left[\dfrac{a(m-x)}{m}\right]$ 都不是整数, 但 $\dfrac{ax}{m}+\dfrac{a(m-x)}{m}=a$ 为整数, 可以使用引理

2.2 同余类运算

1. 设 α 是环 $\mathbb{Z}_m$ 中非零元素. 如果存在 $\mathbb{Z}_m$ 中非零元素 $\beta\left(\beta\neq\overline{0}\right)$, 使得 $\alpha\beta=\overline{0}$, 称 α 是零因子, 证明:
(1) 非零元素的 α 是零因子当且仅当 α 不可逆. 从而 Z_m 由彼此不同的三类元素构成: $\overline{0}$, $\varphi(m)$ 个可逆元和 $m-\varphi(m)-1$ 个零因子;
(2) $\mathbb{Z}_m$ 中没有零因子当且仅当 m 是素数.

解答.

(1) 先证明必要性
假设 α 可逆, 那么 $\exists\beta\neq0$ 使得

$$\beta=\alpha^{-1}\alpha\beta=\alpha^{-1}\overline{0}=\overline{0}$$

矛盾! 因此 α 不可逆
再证明充分性
因为 α 不可逆, 因此 $d=(\alpha,m)>1$, 进而存在 β 使得 $d\beta=\overline{m}=\overline{0}$
于是 $d\dfrac{\alpha}{d}\beta=\overline{0}\Rightarrow\alpha\beta=\overline{0}$, 故 α 是零因子

(2) 先证明必要性

$\mathbb{Z}_m$ 没有零因子, 由 (1) 可知 m 没有非平凡因子, 因此 m 为素数

再证明充分性

因为 m 为素数, 故 m 没有非平凡因子, 因此 $\mathbb{Z}_m$ 中没有零因子

2. (1) 对于环 Z_m 中任何元素 α, m 个 α 相加为 $\bar{0}$.

(2) 设 p 为素数. 对于域 $\mathbb{Z}_p$ 中非零元素 α 和正整数 n, 证明: n 个 α 相加为 $\bar{0}$ 当且仅当 $p \mid n$.

解答.

(1) 因为 $m\alpha \equiv 0 \pmod m$, 故 $m\alpha = \overline{0}$

(2) 充分性由 (1) 已证得, 下证必要性

因为 p 为素数, 因此 α 非零因子, 进而 $\alpha n = 0 \Rightarrow n = \overline{0} \Rightarrow p \mid n$

3. 证明当 p 为奇素数时,

$$2^{p-1} \cdot \left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod p.$$

解答.

由欧拉定理

$$2^{p-1} \equiv 1 \pmod p$$

由威尔逊定理

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv (-1)^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \prod_{k=1}^{\frac{p-1}{2}} (-k+p) \equiv (-1)^{\frac{p-1}{2}} (p-1)! \equiv (-1)^{\frac{p-1}{2}} (-1) \equiv (-1)^{\frac{p+1}{2}} \pmod p$$

两式相乘即得

$$2^{p-1} \cdot \left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod p$$

4. 对于整数 $m \geq 2$, 证明: $(m-1)! \equiv -1 \pmod m$ 当且仅当 m 是素数. (这给出判别 m 是否为素数的一种方法.)

解答.

充分性由威尔逊定理是显然的, 下证必要性

若 m 为合数, 那么存在一对零因子 $\alpha, \beta \in \mathbb{Z}_m$ 使得 $\alpha\beta = 0$, 故 $(m-1)! \equiv 0 \not\equiv -1 \pmod m$

故 m 为素数

5. 证明: 若 $\mathbb{Z}_m^* = \left\{\alpha_1, \cdots, \alpha_{\varphi(m)}\right\}$, 则 $\mathbb{Z}_m^* = \left\{\alpha_1^{-1}, \cdots, \alpha_{\varphi(m)}^{-1}\right\}$. 如何将它转述成同余的语言?

解答.
设 $d = (\alpha_i^{-1}, m)$, 那么 $\dfrac{\alpha_i\alpha_i^{-1} - 1}{m} \in \mathbb{Z}$, 设 $z = \dfrac{\alpha_i\alpha_i^{-1} - 1}{m}$
那么 $\alpha_i\alpha_i^{-1} - mz = 1$, 这说明关于 x, y 的方程 $\alpha_i^{-1}x - my = 1$ 有解, 故 $d \mid 1$, 即 $d = 1$
而 $\alpha_i^{-1} \equiv \alpha_j^{-1} \pmod{m} \Leftrightarrow \alpha_i \equiv \alpha_j \pmod{m}$, 所以 $\left\{\alpha_1^{-1}, \alpha_2^{-1}, \cdots, \alpha_{\varphi(m)}^{-1}\right\}$ 也是模 m 的缩系
转化为同余的语言

$$\alpha_i^{-1}x \equiv 1 \pmod{m} \text{ 有解且 } \alpha_i \neq \alpha_j$$

2.3 欧拉–费马定理

1. 设 n 和 m 是互素的正整数, 证明: $m^{\varphi(n)} + n^{\varphi(m)} \equiv 1 \pmod{mn}$.

解答.
由欧拉定理

$$m^{\varphi(n)} \equiv 1 \pmod{n} \quad \text{以及} \quad n^{\varphi(m)} \equiv 1 \pmod{m}$$

相乘得

$$\left(m^{\varphi(n)} - 1\right)\left(n^{\varphi(m)} - 1\right) \equiv 0 \pmod{mn} \Rightarrow m^{\varphi(n)}n^{\varphi(m)} - m^{\varphi(n)} - n^{\varphi(m)} + 1 \equiv 0 \pmod{mn}$$

显然

$$m^{\varphi(n)}n^{\varphi(m)} \equiv 0 \pmod{mn}$$

上两式相减整理即得

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

2. (1) 对每个与 10 互素的整数 a, 证明: $a^{20} \equiv 1 \pmod{100}$.
(2) 求 3^{193} 的十进制表达式中的个位和十位数字.

解答.
(1) 因为 $(a, 10) = 1$, 故 $(a, 2^2) = (a, 5^2) = 1$, 由欧拉定理得

$$a^{\varphi(4)} \equiv 1 \pmod{4} \Rightarrow a^{20} \equiv 1 \pmod{4} \quad \text{及} \quad a^{\varphi(25)} \equiv 1 \pmod{25} \Rightarrow a^{20} \equiv 1 \pmod{25}$$

又 $(4, 25) = 1$, 两式相乘即得

$$a^{20} \equiv 1 \pmod{100}$$

(2) 由 $3^4 \equiv 1 \pmod{10}$, 于是

$$3^{193} \equiv 3^{3\times 64+1} \equiv 3 \pmod{10}$$

于是 3^{193} 的个位数字为 3

由 $3^{20} \equiv 1 \pmod{100}$ 知

$$3^{193} \equiv 3^{20\times 9+13} \equiv 3^{13} \equiv 23 \pmod{100}$$

于是 3^{193} 的十位数字为 2

3. (1) 设 $a, b \in \mathbb{Z}$, $n \geq 1$, p 为素数. 如果 $a \equiv b \pmod{p^n}$, 证明: 对每个整数 $k \geq 0$, $a^{p^k} \equiv b^{p^k} \pmod{p^{n+k}}$.

(2) 证明: 对每个奇数 a 和 $k \geq 1$, $a^{2^k} \equiv 1 \pmod{2^{k+2}}$.

解答.

(1) 对 k 进行归纳, 当 $k=1$ 时

$$a^p - b^p \equiv (a-b)\left(a^{p-1} + a^{p-2}b + \cdots + b^{p-1}\right) \equiv (a-b)\, pa^{p-1} \pmod{p}$$

于是$p \mid (a^{p-1} + a^{p-2}b + \cdots + b^{p-1})$, 又 $p^n \mid (a-b)$, 于是

$$p^{n+1} \mid (a^p - b^p) \Rightarrow a^p \equiv b^p \pmod{p^{n+1}}$$

假设结论 k 时成立,那么 $k+1$ 时

$$a^{p^{k+1}} - b^{p^{k+1}} \equiv \left(a^{p^k} - b^{p^k}\right)\left(a^{p^{k+1}-p^k} + a^{p^{k+1}-2p^k} b^{p^k} + \cdots + b^{p^{k+1}-p^k}\right) \equiv \left(a^{p^k} - b^{p^k}\right) pa^{p^{k+1}} \pmod{p^{n+k}}$$

故 $a^{p^{k+1}} \equiv b^{p^{k+1}} \pmod{p^{n+k+1}}$

由数学归纳法知, $\forall k \in \mathbb{N}$, 结论成立

(2) 注意到

$$a^{2^k} - 1 \equiv (a^2-1)\left(a^{2^k-2} + a^{2^k-4} + \cdots + a^2 + 1\right) \equiv (a^2-1)\, 2^{k-1} \pmod{2}$$

又 $8 \mid (a^2-1)$, 故 $a^{2^k} \equiv 1 \pmod{2^{k+2}}$

2.4 中国剩余定理

1. 解下列同于方程组:

(1) $32x \equiv 12 \pmod 8$; (2) $28x \equiv 124 \pmod{116}$ (3) $5x \equiv 44 \pmod{81}$.

解答.

(1) 因为 $8 \mid 32$, 因此 $32x \equiv 0 \not\equiv 12 \pmod 8$, 该方程无解

(2) 因为 $(28, 116) = 4 \mid 124$, 故该方程有解, 等价于 $7x \equiv 8 \pmod{29}$

解得 $x \equiv 26 \pmod{29}$

(3) 因为 $(5, 81) = 1 \mid 44$, 故该方程有解, 于是

$$x \equiv \frac{44}{5} \equiv \frac{125}{5} \equiv 25 \pmod{81}$$

2. 解下列同余方程组:

(1) $\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 1 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases}$; (2) $\begin{cases} x \equiv 2 \pmod 4 \\ x \equiv 3 \pmod 5 \\ x \equiv 7 \pmod 9 \end{cases}$.

解答.

(1) $M_1 = 35, M_2 = 21, M_3 = 15; N_1 = 2, N_2 = 1, N_3 = 1$

那么全部解为 $x \equiv 35 \times 2 + 21 + 2 \times 15 \equiv 16 \pmod{105}$

(2) $M_1 = 45, M_2 = 36, M_3 = 20; N_1 = 1, N_2 = 1, N_3 = 5$

那么全部解为 $x \equiv 45 \times 2 + 36 \times 3 + 20 \times 5 \times 7 \equiv 178 \pmod{180}$

3. 用中国剩余定理解同余方程 $37x \equiv 31 \pmod{77}$.

解答.

将方程分解为一个同余方程组

$$\begin{cases} 37x \equiv 31 \pmod 7 \\ 37x \equiv 31 \pmod{11} \end{cases} \Rightarrow \begin{cases} 2x \equiv 3 \pmod 7 \\ 4x \equiv 9 \pmod{11} \end{cases} \Rightarrow \begin{cases} x \equiv 5 \pmod 7 \\ x \equiv 5 \pmod{11} \end{cases}$$

于是方程的解为 $x \equiv 5 \pmod{77}$

4. 求 2^{400} 被 319 除的余数.

解答.

注意到 $2^{140} \equiv 1 \pmod{319}$, 于是

$$2^{400} \equiv 2^{140\times 2+120} \equiv 2^{120} \pmod{319}$$

有 $2^2 \equiv 4 \pmod 4$, $2^4 \equiv 16 \pmod{319}$, $2^8 \equiv 256 \pmod{319}$, $2^{16} \equiv 141 \pmod{319}$, $2^{32} \equiv 103 \pmod{319}$

$2^{64} \equiv 82 \pmod{319}$, 那么

$$2^{120} = 2^{64+32+16+8} \equiv 82 \times 103 \times 141 \times 256 \equiv 111 \pmod{319}$$

即 2^{400} 被 319 除的余数为 111

5. 设 m_1, m_2 是正整数, b_1, $b_2 \in \mathbb{Z}$. 证明: 同于方程组

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \end{cases}$$

有整数解得充分必要条件是 $(m_1, m_2) \mid (b_1 - b_2)$. 并且在此条件成立时, 解为模 $[m_1, m_2]$ 的一个同余类.

解答.

方程等价于存在整数 x, k_1, k_2 满足

$$\begin{cases} x = b_1 + k_1 m_1 \\ x = b_2 + k_2 m_2 \end{cases} \Leftrightarrow k_2 m_2 - k_1 m_1 = b_1 - b_2$$

上述方程有解的充要条件为 $(m_1, m_2) \mid b_1 - b_2$, 且全部解为 $\begin{cases} k_1 = k_1^0 + \dfrac{m_2}{(m_1, m_2)} t \\ k_2 = k_2^0 + \dfrac{m_1}{(m_1, m_2)} t \end{cases}$ $, t \in \mathbb{Z}$, k_1^0, k_2^0 是特解

于是 $x = b_1 + k_1 m_1 = b_1 + m_1 k_1^0 + \dfrac{m_1 m_2}{(m_1, m_2)} t = b_1 + m_1 k_1^0 + [m_1, m_2]\, t$, 即解是 $[m_1, m_2]$ 的一个同余类

6. 设 m_1, m_2 是互素的正整数. 证明:
(1) 若 S_1, S_2 分别是模 m_1 和模 m_2 的完系. 则

$$S=\{m_1x_1+m_2x_2 : x_1\in S_2, x_2\in S_1\}$$

是模 m_1m_2 的完系;
(2) 若 S_1, S_2 分别是模 m_1 和模 m_2 的缩系. 则

$$S=\{m_1x_1+m_2x_2 : x_1\in S_2, x_2\in S_1\}$$

是模 m_1m_2 的缩系.(由此可知 $\varphi(m_1m_2)=\varphi(m_1)\varphi(m_2)$)

解答.
(1) 设 $a, b\in S$, 且 $a=m_1x_1+m_2x_2$, $b=m_1x_1'+m_2x_2'$, 因为

$$a=b\Leftrightarrow m_1(x_1-x_1')+m_2(x_2-x_2')=0\Leftrightarrow x_1=x_1', x_2=x_2', \qquad 其中\ (m_1,m_2)=1$$

故对于不同的 x_1, x_2, $m_1x_1+m_2x_2$ 不相同, 而 x_1, x_2 总共有 m_1m_2 种选择, S 恰好为 m_1m_2 的完系
(2) 由 (1) 类似可知 $m_1x_1+m_2x_2$ 两两不同, 只证 $(m_1x_1+m_2x_2, m_1m_2)=1$
因为 $x_1\in S_2$, $x_2\in S_1$, 于是 $(x_1,m_2)=1$, $(x_2,m_1)=1$, 由 $(m_1,m_2)=1$, 那么 $(x_1m_1,m_2)=1$, $(x_2m_2,m_1)=1$
进而 $(x_1m_1+m_2x_2,m_2)=1$, $(x_2m_2+m_1x_1,m_1)=1$, 于是 $(x_1m_1+m_2x_2,m_1m_2)=1$

7. 设 n 为正整数. 证明: 必有连续 n 个正整数, 其中每个整数均被某个大于 1 的整数的平方所除尽.

解答.
设 $p_1, p_2, \cdots, p_n$ 是 n 个不相同的素数 (素数无限多, 因此一定存在 n 个不同的素数), 考虑下列同余方程组

$$\begin{cases} x\equiv 0 \pmod{p_1^2} \\ x\equiv 1 \pmod{p_2^2} \\ \vdots \\ x\equiv n-1 \pmod{p_n^2} \end{cases}$$

由中国剩余定理其必有解, 记其中一个为 y, 于是 $y-i-1$ 被 $p_i^2 (i=1,2,\cdots,n)$ 整除
$y-n+1$, $y-n$, $\cdots$, y 这连续 n 个整数满足条件

3 原根和指数

3.1 原根

1. 设 $m \geq 2$, 整数 a 和 b 模 m 的阶为 s 和 t, 并且 $(s,t)=1$. 证明: ab 模 m 的阶为 st.

解答.
设 ab 模 m 的阶为 r, 那么 $(ab)^r \equiv 1 \pmod{m}$, 于是

$$1 \equiv (ab)^{rs} \equiv b^{rs} \pmod{m}$$

于是 $t \mid rs \Rightarrow t \mid r$, 同理 $s \mid r$, 于是 $st \mid r$, 又

$$(ab)^{st} \equiv (a^s)^t \left(b^t\right)^s \equiv 1 \pmod{m}$$

故 $r = st$

2. a 对模 m 和模 n 的阶分为 s 和 t, 证明: a 对模 $[m,n]$ 的阶为 $[s,t]$.

解答.
设 a 对模 $[m,n]$ 的阶为 r, 那么

$$a^r \equiv 1 \pmod{[m,n]} \text{ 或 } a^r \equiv 1 \pmod{[m,n]}$$

那么

$$a^r \equiv 1 \pmod{m} \text{ 且 } a^r \equiv 1 \pmod{n}$$

于是 $s \mid r$ 且 $t \mid r$, 进而 $s \mid [s,t]$, 又

$$a^s \equiv 1 \pmod{m} \text{ 且 } a^t \equiv 1 \pmod{n} \Rightarrow a^{[s,t]} \equiv 1 \pmod{m} \text{ 且 } a^{[m,n]} \equiv 1 \pmod{n} \Rightarrow a^{[m,n]} \equiv \pmod{[m,n]}$$

故 a 对模 $[m,n]$ 的阶为 $[s,t]$

3. 设 p 为奇素数, 若 g 是模 p 的原根. 求 $-g$ 模 p 的阶.

解答.
因为

$$-g \equiv g^{1+\frac{p-1}{2}} \equiv g^{\frac{p+1}{2}} \pmod{p}$$

故 $-g$ 的阶为

$$\frac{p-1}{\left(\frac{p+1}{2},p-1\right)}=\begin{cases}p-1, & p\equiv 1 \pmod 4\\ \dfrac{p-1}{2}, & p\equiv 3 \pmod 4\end{cases}$$

题目3的注记.

[1] $g^{\frac{p-1}{2}}\equiv -1 \pmod p$ 的证明: 设 $g^r\equiv -1 \pmod p$, 若 $r<\dfrac{p-1}{2}$, 那么 $g^{2r}\equiv 1 \pmod p$, 而 $2r<p-1$, 这与 g 是模 p 的原根矛盾, 故 $p-1\le 2r\le 2(p-2)$, 又 $p-1\mid 2r$, 故 $2r=p-1\Rightarrow r=\dfrac{p-1}{2}$

4. (1) 对于 $p=5, 7, 11, 13, 23$, 求模 p 的最小正原根.

(2) 求模 7^2 的全部原根.

解答.

(1) 最小正原根分别为 2, 3, 2, 2, 5

(2) 因为 $\varphi(7^2)=42$, 有因子 2, 3, 7, 验算知 3 是模 7^2 的原根

$\varphi(42)=12$, 于是模 7^2 的原根有 12 个, 42 的缩系为 1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41

7^2 的全部原根为 $2^1, 2^5, 2^{11}, 2^{13}, 2^{17}, 2^{19}, 2^{23}, 2^{25}, 2^{29}, 2^{31}, 2^{37}, 2^{41}$

即 3, 5, 10, 12, 17, 24, 26, 33, 38, 40, 45, 47

5. 若 n 和 a 均是正整数, $a\ge 2$. 证明: $n\mid\varphi(a^n-1)$.

解答.

考虑方程

$$a^x\equiv 1 \pmod{a^n-1}$$

显然 n 是其最小正整数解, 另一方面, 因为 $(a^n-1,a)=1$, 于是由欧拉定理

$$a^{\varphi(a^n-1)}\equiv 1 \pmod{a^n-1}$$

因此 $n\mid\varphi(a^n-1)$

6. 如果 $n\ge 2$, 证明: $n\nmid 2^n-1$.

解答.

若 n 是偶数, 那么 $(2,n)=2>1$, 那么不存在 s 使得 $2^s\equiv 1 \pmod n$, 即 $n\nmid 2^n-1$

若 n 是奇数, 设 p 是 n 的最小素因子, 又设 r 是 2 模 p 的阶

反证, 假设 $n \mid 2^n - 1$, 那么 $p \mid 2^n - 1$, 进而 $r \mid n$, 又 $r \mid \varphi(p) = p - 1$

故 $r \mid (n, p-1) = 1$, 因此 $r = 1$, 矛盾!

7. 设 p 是奇素数, $n \geq 1$. 证明:

$$\sum_{k=1}^{p-1} k^n \equiv \begin{cases} -1 \pmod p, & \text{如果 } p-1 \mid n, \\ 0 \pmod p, & \text{如果 } p-1 \nmid n. \end{cases}$$

解答.

1° 若 $p-1 \mid n$, 又 $(k,p) = 1$, $k = 1, 2, \cdots, p-1$, 于是

$$k^{\varphi(p)} \equiv 1 \pmod p \Rightarrow k^n \equiv 1 \pmod p$$

那么

$$\sum_{k=1}^{p-1} k^n \equiv p - 1 \equiv -1 \pmod p$$

2° 若 $p-1 \nmid n$

记模 p 的一原根为 g, 因为 $p-1 \nmid n$, 那么 $g^n \not\equiv 1 \pmod p$, 于是

$$\sum_{k=1}^{p-1} k^n \equiv \sum_{k=1}^{p-1} g^{kn} \equiv \frac{g^n\left(g^{(p-1)n} - 1\right)}{g^n - 1} \equiv 0 \pmod p$$

8. 8.(1) 设 $F_n = 2^{2^n} + 1$, $n \geq 1$. 证明: F_n 的每个素因子都有形式 $2^{n+1}x + 1\,(x \in \mathbb{Z})$.

(2) 对于任意给定的整数 $l \geq 1$, 证明: 有无穷多个素数模 2^l 余 1.

解答.

(1) 设 p 是 F_n 的素因子, 那么

$$2^{2^n} \equiv -1 \pmod p \Rightarrow 2^{2^{n+1}} \equiv 1 \pmod p$$

记 r 为 2 模 p 的阶, 由上式 $r \nmid 2^n$ 且 $r \mid 2^{n+1}$, 故 $r = 2^{n+1}$, 那么

$$2^{2^{n+1}} \equiv 1 \pmod p$$

即 $p = 2^{n+1}x + 1\,(x \in \mathbb{Z})$

(2) 即证存在无穷多个形如 $2^l x + 1\,(x \in \mathbb{Z})$ 的素数, 考察 $F_k\,(k \geq l-1)$ 的素因子

由 (1) F_k 的素因子都应该具有

$$2^{k+1}x + 1 = 2^l\left(2^{k+1-l}x\right) + 1 = 2^l x' + 1\left(x' = 2^{k+1-l}x \in \mathbb{Z}\right)$$

的形式, 而熟知费马数两两互素, 因此这些素因子两两不同

9. (1) 设 p 为奇素数, $a \geq 2$. 证明: 若 $a^p - 1$ 的素因子 q 不整除 $a-1$, 则必有形式 $q = 2px+1\,(x \in \mathbb{Z})$.
(2) 设 p 为给定的奇素数, 证明: 形如 $2px+1\,(x \in \mathbb{Z})$ 的素数有无限多个.

解答.
(1) p 是奇素数, 又 $q \nmid a-1$, 于是 p 是 a 模 q 的阶, 因此 $p \mid \varphi(q) = q-1$, 又 p 是奇数, $q-1$ 是偶数, 于是 $2p \mid q-1$, 即 q 有 $2px+1$ 的形式
(2) 假设这样的素数仅有有限个, 设为 $p_1, p_2, \cdots, p_r$, 取 $P = (2p_1p_2\cdots p_r)^p - 1$, 记 $g = 2p_1\cdots p_r$, 那么 $g^p \equiv 1 \pmod{P}$, 于是 $p \mid \varphi(P)$, 因为 φ 是积性函数, 所以存在 P 的素因子 q 满足 $p \mid q-1$, 也就是 q 是 $2px+1$ 型的, 而 $P = (2p_1p_2\cdots p_r)^p - 1$, 这说明 q 不是 $p_1, \cdots, p_r$ 中的任何一个, 矛盾!

3.2 指数

1. 解同余方程:
(1) $x^8 \equiv 3 \pmod{13}$; (2) $x^8 \equiv 3 \pmod{143}$; (3)$7^x \equiv 4 \pmod{17}$.

解答.
(1) 首先 2 是模 13 的原根, 且 $2^4 \equiv 3 \pmod{13}$, 再设 $x \equiv 2^y \pmod{13}$于是

$$2^{8y} \equiv 2^4 \pmod{13} 8y-4 \equiv 0 \pmod{12} \Rightarrow y \equiv 2 \pmod{3} \Rightarrow x \equiv 4, 6, 7, 9 \pmod{13}$$

(2) 转化为两个同余方程 $x^8 \equiv 3 \pmod{13}$ 和 $x^8 \equiv 3 \pmod{11}$, 前者已在 (1) 中解决, 考虑后者
首先 2 是模 11 的一个原根, 设 $x \equiv 2^y \pmod{11}$, 那么

$$2^{8y} \equiv 2^8 \pmod{11} \Rightarrow 2^{8y-8} \equiv 1 \pmod{11} \Rightarrow 8y-8 \equiv 0 \pmod{10} \Rightarrow y \equiv 1 \pmod{5} \Rightarrow x \equiv 2, 9 \pmod{11}$$

于是共有八个解, 分别是模 13 和模 11 的解两两组成的方程组的解, 即 $x \equiv 9, 20, 35, 46, 97, 108, 123, 134 \pmod{143}$
(3) $x \equiv 4 \pmod{16}$

2. (1) 写出模 37 的全部 8 次剩余和 15 次剩余.
(2) 写出模 11 的全部二次剩余.

解答.

(1) 1, 6, 8, 10, 11, 14, 23, 26, 27, 29, 31, 36

(2) 首先 2 是模 11 的一个原根, 于是所有的二次剩余为 $2^0, 2^2, 2^4, 2^6, 2^8$, 即 1, 3, 4, 5, 9

3. 设 p 为素数, $p \equiv 2 \pmod 3$, a 和 b 是整数. 证明:

$$a^3 \equiv b^3 \pmod p$$

当且仅当 $a \equiv b \pmod p$.

解答.

充分性显然, 下证必要性

考虑三次同余方程 $x^3 \equiv b^3 \pmod p$, $d = (3, \varphi(p)) = (3, 3k+1) = 1$, 故其有唯一解

而由题 a, b 都是该方程的解, 于是 $a \equiv b \pmod p$

4. 设 p 为奇素数, 整数 a 模 p 的阶为 3. 求 $\dfrac{a}{a+1}$ 模 p 的阶.

解答.

只需求 $\left(\dfrac{a}{a+1}\right)^{-1}$ 的阶, 而 $\left(\dfrac{a}{a+1}\right)^{-1} = a^{-1}(1+a) = 1 + a^{-1} = 1 + a^2$

设 $1+a^2$ 的阶为 $r = 2s+t$, $0 \le t < 2$, 由题 $a^3 \equiv 1 \pmod p$ 且 $a \not\equiv 1 \pmod p$, 那么

$$\begin{aligned}
\left(1+a^2\right)^r &= \left(1+a^2\right)^{2s}\left(1+a^2\right)^t \\
&= \left(a^4+2a^2+1\right)^s\left(1+a^2\right)^t \\
&= \left(a+2a^2+1\right)^s\left(1+a^2\right)^t \\
&= a^{2s}\left(1+a^2\right)^t
\end{aligned}$$

若 $t = 1$, 那么

$$a^{2s}\left(1+a^2\right)^t = \begin{cases} 1+a^2 = -a \neq 1, & s \equiv 0 \pmod 3 \\ a^2+a = -1 \neq 1, & s \equiv 1 \pmod 3 \\ 1+a = -a^2 \neq 1, & s \equiv 2 \pmod 3 \end{cases}$$

于是 $t = 0$, 那么 $a^{2s} \equiv 1 \pmod p$, 于是 $3 \mid 2s \Rightarrow 3 \mid s$, 于是 $s = 3$, $r = 6$, 即 $\dfrac{a}{a+1}$ 模 p 的阶为 6

4　二次剩余

4.1　勒让德符号

1.　设 p 为奇素数, a, $b \in \mathbb{Z}$, $(a,p)=1$. 证明:

$$\sum_{n=0}^{p-1}\left(\frac{an+b}{p}\right)=0.$$

解答.

因为 $(a,p)=1$, 于是 b, $a+b$, $\cdots$, $a\,(p-1)+b$ 构成了模 p 的一个完系, 故

$$\sum_{n=0}^{p-1}\left(\frac{an+b}{p}\right)=\sum_{n=0}^{p-1}\left(\frac{n}{p}\right)=0$$

2.　设 p 是奇素数, n 是最小正整数使得 $\left(\frac{n}{p}\right)=-1$, 证明: n 为素数.

解答.

设 n 有标准分解 $n=p_1^{\alpha_i}\cdots p_k^{\alpha}$, 于是

$$-1=\left(\frac{n}{p}\right)=\left(\frac{p_i}{p}\right)^{\alpha_i}\cdots\left(\frac{p_k}{p}\right)^{\alpha_k}$$

因此, 必存在正整数 j 使得 $\left(\frac{p_j}{p}\right)=-1$, 否则 $\forall i\in\{1,2,\cdots,k\}$ 有 $\left(\frac{p_i}{p}\right)=1$, 那么

$$\left(\frac{p_i}{p}\right)^{\alpha_i}\cdots\left(\frac{p_k}{p}\right)^{\alpha_k}=1\neq-1$$

矛盾! 那么 $\left(\frac{p_j}{p}\right)=-1$, 而 $p_j\leq n$, 因此 $p_j=n$, 故 n 为素数

3.　证明形如 $8m+3$, $8m+5$, $8m+7$ 的素数均有无限多个.

解答.

1° 显然这样的素数是存在的, 并假设这样的素数仅有有限个, 设为 p_1, $\cdots$, p_r, 考虑正整数 $n=(p_1\cdots p_r)^2+2$, n 为奇数, 那么 n 的素因子全为奇素数, 任取一个, 记为 p, 于是

$$0\equiv n\equiv(p_1\cdots p_r)^2+2\pmod p$$

这说明 $(p_1\cdots p_r)^2\equiv -2 \pmod p$, 于是 $p\equiv 1 \pmod 8$ 或 $p\equiv 3 \pmod 8$, 而

$$(p_1\cdots p_r)^2+2\equiv 3^{2r}+2\equiv 3 \pmod 8$$

于是 n 的素因子不可能全为 $8k+1$ 型, 否则 $n\equiv 1 \pmod 8$, 与上式矛盾! 那么一定存在一个素因子 $q\equiv 3 \pmod 8$, 而 q 不是 $p_1,\cdots,p_r$ 中的任意一个, 因此 $8m+3$ 型的素数有无限多个

2° 显然这样的素数是存在的, 并假设这样的素数仅有有限个, 设为 $p_1,\cdots,p_r$, 考虑正整数 $n=4(p_1\cdots p_r)^2+1$, n 为奇数, 那么 n 的素因子全为奇数, 任取一个, 记为 p, 于是

$$0\equiv n\equiv (2p_1\cdots p_r)^2+1 \pmod p$$

这说明 $(2p_1\cdots p_r)^2\equiv -1 \pmod p$, 那么 $p\equiv 1 \pmod 8$ 或 $p\equiv 5 \pmod 8$ 而

$$(2p_r\cdots p_r)^2+1\equiv 4\cdot 5^{2r}+1\equiv 5 \pmod 8$$

于是 n 的素因子不可能全为 $8k+1$ 型, 否则 $n\equiv 1 \pmod 8$, 与上式矛盾! 那么一定存在一个素因子 $q\equiv 5 \pmod 8$, 而 q 不是 $p_1,\cdots,p_r$ 中的任意一个, 因此 $8m+5$ 型的素数有无限多个

3° 显然这样的素数是存在的, 并假设这样的素数仅有有限个, 设为 $p_1,\cdots,p_r$, 考虑正整数 $n=(p_1\cdots p_r)^2-2$, n 为奇数, 那么 n 的素因子全为奇数, 任取一个, 记为 p, 于是

$$0\equiv n\equiv (p_1\cdots p_r)^2-2 \pmod p$$

这说明 $(2p_1\cdots p_r)^2\equiv 2 \pmod p$, 那么 $p\equiv 1 \pmod 8$ 或 $p\equiv 7 \pmod 8$ 而

$$(p_r\cdots p_r)^2-1\equiv 7^{2r}-2\equiv -1 \pmod 8$$

于是 n 的素因子不可能全为 $8k+1$ 型, 否则 $n\equiv 1 \pmod 8$, 与上式矛盾! 那么一定存在一个素因子 $q\equiv 7 \pmod 8$, 而 q 不是 $p_1,\cdots,p_r$ 中的任意一个, 因此 $8m+7$ 型的素数有无限多个

4. 设 p 为奇素数. 证明: 有无穷多的素数是模 p 的二次非剩余.

解答.

对于任意的正整数 n, 总可以取到 n 个不为 p 的素数, $p_1,p_2,\cdots,p_n$, 再取模 p 的一个非二次剩余 g, 考虑同余方程组

$$\begin{cases} n\equiv g \pmod p \\ n\equiv 1 \pmod{p_i}, \quad i=1,2\cdots,n \end{cases}$$

由中国剩余定理, 该同余方程组有解, 那么

$$\left(\frac{n}{p}\right)=\left(\frac{g}{p}\right)=-1$$

故 n 有素因子 p_j 使得 $\left(\dfrac{p_j}{p}\right)=-1$, 而 p_j 不是 $p_1,\cdots,p_n$ 中的任意一个
$n=1$ 时, 可知模 p 有素非二次剩余, 那么假设模 p 仅有有限个, 记为 $q_1,q_2,\cdots,q_r$, 再取 $n=r$, 并令 $p_i=q_i$, 则由上述结论知存在不同于 $q_1,q_2,\cdots,q_r$ 的二次非剩余, 因此有无穷多的素数是模 p 的二次非剩余

5. 设 p 和 $q=2p+1$ 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 q 的原根.

解答.
(1) 因为 $p\equiv 1 \pmod 4$, 所以 $q\equiv 3 \pmod 8$, 因此 2 是模 q 的二次非剩余, 取 q 的一原根 g, 那么 $\exists i\in\mathbb{N}_+$ 使得 $g^{2i-1}\equiv 2 \pmod p$, 因此 2 模 q 的阶为

$$\frac{q-1}{(q-1,2i-1)}=\frac{q-1}{(2p,2i-1)}=\frac{q-1}{(p,2i-1)}=\varphi(q)$$

因此 2 是模 q 的原根
(2) 因为 $p\equiv 3 \pmod 4$, 所以 $q\equiv -1 \pmod 8$, 因此 -2 是模 q 的二次非剩余, 取 q 的一原根 g, 那么 $\exists i\in\mathbb{N}_+$ 使得 $g^{2i-1}\equiv -2 \pmod p$, 因此 -2 模 q 的阶为

$$\frac{q-1}{(q-1,2i-1)}=\frac{q-1}{(2p,2i-1)}=\frac{q-1}{(p,2i-1)}=\varphi(q)$$

因此 -2 是模 q 的原根

6. 设 p 为素数, $p\equiv 3 \pmod 4$. 记 $q=2p+1$. 则 q 为素数当且仅当 $q\mid 2^p-1$.

解答.
先证必要性, 因为 $p\equiv 3 \pmod 4$, 于是 $q\equiv -1 \pmod 8$, 于是 2 是 q 的二次剩余, 取 q 的一原根 g, 那么 $\exists i\in\mathbb{N}_+$ 使得 $g^{2i}\equiv 2 \pmod p$, 于是

$$2^p\equiv\left(g^{2p}\right)^i\equiv 1 \pmod q$$

即 $q\mid 2^p-1$
再证充分性, 记 r 为 2 模 q 的阶, 那么 $r\mid p$, 因此 $r=p$, 于是 $p\mid\varphi(q)$, 而 $\varphi(q)\le q-1=2p$, 又 $\varphi(q)$ 为偶数, 于是 $\varphi(q)=2p=q-1$, 故 q 为素数

7. 设 p 为奇素数. 证明:

$$\prod_{\substack{r=1 \\ \left(\frac{r}{p}\right)=1}}^{p-1} r \equiv -\left(\frac{-1}{p}\right) \pmod{p}.$$

解答.

因为 $1^2, 2^2, \cdots, \left(\frac{p-1}{2}\right)^2$ 是模 p 的全部二次剩余, 以及威尔逊定理和二次剩余的欧拉判别法, 所以

$$\prod_{\substack{r=1 \\ \left(\frac{r}{p}\right)=1}}^{p-1} r \equiv \left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv (-1)^{\frac{p-1}{2}}(p-1)! \equiv -(-1)^{\frac{p-1}{2}} \equiv -\left(\frac{-1}{p}\right) \pmod{p}$$

8. 设 p 为素数,

(1) 若 $p \equiv 1 \pmod{4}$, 则

$$\sum_{\substack{r=1 \\ \left(\frac{r}{p}\right)=1}}^{p-1} r = \frac{p(p-1)}{4}, \quad \sum_{a=1}^{p-1} a\left(\frac{a}{p}\right) = 0;$$

(2) 若 $p \equiv 3 \pmod{4}$, 并且 $p \geq 7$, 则

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

解答.

(1) 因为 $p \equiv 1 \pmod{4}$, 那么, 若 $\left(\frac{k}{p}\right) = 1$, 则

$$\left(\frac{-k}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{k}{p}\right) = 1$$

于是

$$2\sum_{\substack{r=1 \\ \left(\frac{r}{p}\right)=1}}^{p-1} r = \sum_{\substack{r=1 \\ \left(\frac{r}{p}\right)=1}}^{p-1} k + (p-k) = \frac{p(p-1)}{2} \Rightarrow \sum_{\substack{r=1 \\ \left(\frac{r}{p}\right)=1}}^{p-1} r = \frac{p(p-1)}{4}$$

进而

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

(2) 取 p 的一个原根 g, 那么

$$\sum_{\substack{r=1\\ \left(\frac{r}{p}\right)=1}}^{p-1} r\equiv\sum_{k=0}^{\frac{p-3}{2}} g^{2k}\equiv\frac{g^{p-1}-1}{g^2-1}\equiv 0 \pmod p$$

以及

$$\sum_{a=1}^{p-1} a\left(\frac{a}{p}\right)\equiv\sum_{a=0}^{p-2}(-g)^a\equiv\frac{1-g^{p-1}}{1+g}\equiv 0 \pmod p$$

4.2　二次互反律

1.　计算 $\left(\frac{17}{23}\right)$, $\left(\frac{19}{37}\right)$, $\left(\frac{92}{101}\right)$.

解答.

(1) $\left(\frac{17}{23}\right)=\left(\frac{23}{17}\right)=\left(\frac{6}{17}\right)=-1$

(2) $\left(\frac{19}{37}\right)=\left(\frac{-1}{19}\right)=-1$

(3) $\left(\frac{92}{101}\right)=\left(\frac{3^2}{101}\right)=1$

2.　确定以 a 为二次剩余的素数, 其中 $a=-3$, 5, 15.

解答.

1° $a=-3$

$$\left(\frac{-3}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}}=\begin{cases}1, & p\equiv 1,7 \pmod{12}\\ -1. & p\equiv 5,11 \pmod{12}\end{cases}$$

2° $a=5$

$$\left(\frac{5}{p}\right)=\left(\frac{p}{5}\right)(-1)^{\frac{p-1}{2}}=\begin{cases}1, & p\equiv 1,3,7,9 \pmod{20}\\ -1, & p\equiv 11,13,17,19 \pmod{20}\end{cases}$$

3° $a=15$

$$\left(\frac{15}{p}\right)=\left(\frac{3}{p}\right)\left(\frac{5}{p}\right)=1,\quad p\equiv 1,7,11,17,43,49,53,59 \pmod{60}$$

3. 设 $p=4k+1$ 是素数, a 是 k 的因子, 证明 $\left(\frac{a}{p}\right)=1$.

解答.

只需证明对于 k 的任何素因子 q, 总有 $\left(\frac{q}{p}\right)=1$, 这是因为

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

4. 若 $p=10m-1$ 为素数, 证明 $p \mid 5^{5m-1}-1$.

解答.

由二次互反律

$$\left(\frac{5}{p}\right)=\left(\frac{p}{5}\right)=\left(\frac{-1}{5}\right)=1$$

因此 $5=g^{2i}$, 其中 g 是模 p 的原根, i 是某个正整数, 那么

$$5^{5m-1}\equiv g^{10m-2}\equiv 1 \pmod p$$

即 $p \mid 5^{5m-1}-1$

5. 设 $n\geq 2$, $p=2^n+1$ 为素数. 证明:

(1) 对每个 $a\in\mathbb{Z}$, a 为模 p 的原根当且仅当 $\left(\frac{a}{p}\right)=-1$;

(2) 证明 3 和 7 均为模 p 的原根.

解答.

(1) 必要性显然, 下证充分性

取模 p 一原根 g, 那么 $\left(\frac{a}{p}\right)=-1\Leftrightarrow a=g^{2i-1}$, i 是某一正整数, 于是 a 模 p 的阶为

$$\frac{p-1}{(p-1,2i-1)}=\frac{2^n}{(2^n,2i-1)}=2^n=p-1$$

于是所有的二次非剩余都是原根

(2) 1° 因为 $p=2^n+1$ 为素数, 因此 $p\equiv 2 \pmod 3$, 于是

$$\left(\frac{3}{p}\right)=\left(\frac{p}{3}\right)=\left(\frac{2}{3}\right)=-1$$

于是由 (1) 中结论, 3 是模 p 的原根

2° 首先 n 不为奇数, 否则设 $n=st$, 其中 s,t 是 n 的奇因子, 那么

$$p=2^{st}+1=(2^s+1)\left(2^{s(t-1)}-2^{s(t-2)}+\cdots+1\right)$$

这与 p 为素数矛盾, 那么 $p=2^n+1$ 模 7 的正剩余可能为 3, 5, 而 $\left(\frac{3}{7}\right)=\left(\frac{5}{7}\right)=-1$, 于是

$$\left(\frac{7}{p}\right)=\left(\frac{p}{7}\right)=-1$$

于是由 (1) 中结论, 7 是模 p 的原根

6. (1) 设 $n=2^m a+1$, 其中 $m\ge 2$, $1\le a<2^m$. 如果 p 为奇素数, 并且 $\left(\frac{n}{p}\right)=-1$, 证明: n 是素数当且仅当 $p^{\frac{n-1}{2}}\equiv -1 \pmod{n}$.
(2) 设 $n=2^m+1$, $m\ge 2$. 证明: n 为素数当且仅当 $3^{\frac{n-1}{2}}\equiv -1 \pmod{n}$.

解答.
(1) 先证明必要性
由二次互反律

$$\left(\frac{p}{n}\right)=\left(\frac{n}{p}\right)(-1)^{\frac{p-1}{2}\frac{n-1}{2}}=\left(\frac{n}{p}\right)=-1$$

于是 $p=g^{2i-1}$, 其中 g 是模 n 的一个原根, i 是某个正整数, 那么

$$p^{\frac{n-1}{2}}\equiv g^{(n-1)i-\frac{n-1}{2}}\equiv g^{\frac{n-1}{2}}\equiv -1 \pmod{n}$$

再证明充分性
任取 n 的一个素因子 q, q 一定为奇因子, 令 r 为 p 模 q 的阶, 因为 $p^{\frac{n-1}{2}}\equiv -1 \pmod{n}$, 于是 $p^{2^{m-1}a}\equiv -1 \pmod{q}$, 以及 $p^{2^m a}\equiv 1 \pmod{q}$, 那么 $d\mid 2^m a$ 且 $d\nmid 2^{m-1}a$, 于是 $2^m\mid d\mid 2^m a$, 又 $d\mid q-1$, 于是 $2^m\mid q-1$, 那么

$$q^2\ge (2^m+1)^2=2^{2m}+2^{m+1}+1>2^m a+1\Rightarrow q>\sqrt{n}$$

于是 n 的每个素因子都大于 $\sqrt{n}$, 故 n 为素数
(2) 由 (1), 只需证明 $\left(\frac{n}{3}\right)=-1$, 因为 $n=2^m+1$ 为素数, 因此 m 不可能含有奇因子, 那么 $m=2^k$, 那么 $n=2^m+1\equiv 0, 2 \pmod{3}$, 而 0, 2 都是 3 的二次非剩余, 从而 $\left(\frac{n}{3}\right)=-1$

4.3 二次同余方程

1. 解下列同余方程:
(1) $2x^2+3x+1\equiv 0 \pmod{28}$; (2) $x^2\equiv -1 \pmod{169}$;
(3) $x^2\equiv 2 \pmod{98}$; (4) $3x^2+x+6\equiv 0 \pmod{45}$.

解答.

(1) 将其分解为两个同余方程

$$\begin{cases}2x^2+3x+1\equiv 0 \pmod 4\\ 2x^2+3x+1\equiv 0 \pmod 7\end{cases}$$

对于 $2x^2+3x+1\equiv 0 \pmod 4$, 先考虑 $2x^2+3x+1\equiv 0 \pmod 2 \Rightarrow x\equiv -1 \pmod 2 \Rightarrow x\equiv 1,3 \pmod 4$, 依次验证知 $x\equiv 3 \pmod 4$ 是解; 对于 $2x^2+3x+1\equiv 0 \pmod 7$, 那么

$$2\left(x^2+\frac{3}{2}x+\frac{1}{2}\right)\equiv 0 \pmod 7 \Rightarrow x^2+5x+4\equiv 0 \pmod 7 \Rightarrow \left(x+\frac{5}{2}\right)^2\equiv\left(\frac{3}{2}\right)^2 \pmod 7$$

解得 $x\equiv 3,6 \pmod 7$, 于是原方程解为

$$\begin{cases}x\equiv 3 \pmod 4\\ x\equiv 3 \pmod 7\end{cases} \Rightarrow x\equiv 3 \pmod{28} \text{ 以及 } \begin{cases}x\equiv 3 \pmod 4\\ x\equiv 6 \pmod 7\end{cases} \Rightarrow x\equiv 27 \pmod{28}$$

故该同余方程的解为 $x\equiv 3,\ 27 \pmod{28}$

(2) 先考虑同余方程 $x^2\equiv -1 \pmod{13} \Rightarrow x\equiv \pm 5 \pmod{13}$, 设 $x=5+13y$ 是 $x^2\equiv -1 \pmod{169}$ 的解, 那么

$$(5+13y)^2\equiv 130y+25\equiv -1 \pmod{169} \Rightarrow 10y+2\equiv 0 \pmod{13} \Rightarrow y\equiv 5 \pmod{13}$$

于是 $x\equiv 70 \pmod{169}$ 是方程的一个解, 进而所有解为 $x\equiv \pm 70 \pmod{169}$, 即 $x\equiv 70,\ 99 \pmod{169}$

(3) 将其分解为两个同余方程

$$\begin{cases}x^2\equiv 2 \pmod 2\\ x^2\equiv 2 \pmod{49}\end{cases} \Rightarrow \begin{cases}x\equiv 0 \pmod 2\\ x\equiv 10 \pmod{49}\end{cases} \text{ 及 } \begin{cases}x\equiv 0 \pmod 2\\ x\equiv -10 \pmod{49}\end{cases} \Rightarrow x\equiv 10,88 \pmod{98}$$

(4) 将其分解为两个同余方程

$$\begin{cases}3x^2+x+6\equiv 0 \pmod 5\\ 3x^2+x+6\equiv 0 \pmod 9\end{cases}$$

对于 $3x^2+x+6\equiv 0 \pmod 5$, 有

$$3x^2+x+6\equiv 3\left(x^2+\frac{1}{3}x+2\right)\equiv x^2+2x+2\equiv 0 \pmod 5 \Rightarrow (x+1)^2\equiv 2^2 \pmod 5 \Rightarrow x\equiv 1,2 \pmod 5$$

对于 $3x^2+x+6\equiv 0 \pmod 9$, 先考虑 $3x^2+x+6\equiv 0 \pmod 3 \Rightarrow x\equiv 0 \pmod 3 \Rightarrow x\equiv 0,\ 3,\ 6 \pmod 9$, 依次验证知解为 $x\equiv 3 \pmod 9$, 于是方程的解为

$$\begin{cases}x\equiv 1 \pmod 5\\ x\equiv 3 \pmod 9\end{cases} \Rightarrow x\equiv 21 \pmod{45} \text{ 以及 } \begin{cases}x\equiv 2 \pmod 5\\ x\equiv 3 \pmod 9\end{cases} \Rightarrow x\equiv 12 \pmod{45}$$

故该同余方程的解为 $x \equiv 12, 21 \pmod{45}$

2. 设 $f(x, y)$ 是关于 x, y 的整系数多项式. $(x, y) = (a, b)$ 和 (c, d) 均是同余方程 $f(x, y) \equiv 0 \pmod{m}$ 的整数解, 即 $f(a, b) \equiv 0 \pmod{m}$, $f(c, d) \equiv 0 \pmod{m}$. 称这两组解为模 m 的同一个解, 是指 $a \equiv c \pmod{m}$, 并且 $b \equiv d \pmod{m}$.

(1) 设 p 为奇素数, a 为整数. 证明: 同余方程

$$x^2 - y^2 \equiv a \pmod{p}$$

的模 p 解数为 $p-1$ (若 $p \nmid a$) 或 $2p-1$ (若 $p \mid a$).

(2) 证明:

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

解答.

(1) 若 $p \mid a$, 方程即为 $x^2 \equiv y^2 \pmod{p}$, $y = 0$ 时, 方程有一解, 当 y 为模 p 剩余系中其余数时, 其必有两解, 故总共有解 $2p-1$ 个; 若 $p \nmid a$, 做变换 $u = x - y$, $v = x + y$, 那么

$$uv \equiv a \pmod{p}$$

因为 $(x, y) \mapsto (u, v)$ 是一个双射, 故该方程的解数就是原方程的解数, $u = 0$ 时方程无解; 对于任意的 $u \in \mathbb{Z}_p^*$, 其总有解 $v \equiv \dfrac{a}{u} \pmod{p}$, 故解数为 $\left|\mathbb{Z}_p^*\right| = p - 1$

(2) 下面用另一种方式导出同余方程 $x^2 - y^2 \equiv a \pmod{p}$ 的解数, 首先固定 y, 那么 $x^2 \equiv y^2 + a \pmod{p}$ 的解数为 $\left(\dfrac{y^2+a}{p}\right) + 1$ 个, 再让 y 遍历 $\mathbb{Z}_p$, 故总的解数为 $\displaystyle\sum_{y=0}^{p-1} 1 + \left(\frac{y^2+a}{p}\right)$, 再由 (1) 得

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

3. 设 p 为奇素数, $a, b, c \in \mathbb{Z}$, $p \nmid a$, $D = b^2 - 4ac$. 证明:

$$\sum_{x=0}^{p-1} \left(\frac{ax^2+bx+c}{p}\right) = \begin{cases} -\left(\dfrac{a}{p}\right), & p \nmid D, \\ (p-1)\left(\dfrac{a}{p}\right), & p \mid D. \end{cases}$$

解答.

当 x 遍历模 p 的完系时, $x+\dfrac{b}{2a}$ 也会遍历模 p 的完系, 于是

$$\begin{aligned}\sum_{x=0}^{p-1}\left(\frac{ax^2+bx+c}{p}\right)&=\sum_{x=0}^{p-1}\left(\frac{a\left(x+\dfrac{b}{2a}\right)^2-\dfrac{b^2-4ac}{4a^2}}{p}\right)\\&=\sum_{x=0}^{p-1}\left(\frac{ax^2+d}{p}\right)\\&=\sum_{x=0}^{p-1}\left(\frac{a\left(x^2+da^{-1}\right)}{p}\right)\\&=\left(\frac{a}{p}\right)\sum_{x=0}^{p-1}\left(\frac{x^2+da^{-1}}{p}\right)\end{aligned}$$

其中 $d=-\dfrac{D}{4a^2}$, 显然 $p\mid D\Leftrightarrow p\mid da^{-1}$, 于是根据上一题结论知

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

于是

$$\sum_{x=0}^{p-1}\left(\frac{ax^2+bx+c}{p}\right)=\left(\frac{a}{p}\right)\sum_{x=0}^{p-1}\left(\frac{x^2+da^{-1}}{p}\right)=\begin{cases}-\left(\dfrac{a}{p}\right), & p\nmid D,\\ (p-1)\left(\dfrac{a}{p}\right), & p\mid D.\end{cases}$$

4. 设 $a,b,c\in\mathbb{Z}$, $p\nmid ab$, 则同余方程

$$ax^2+by^2\equiv c\pmod p$$

模 p 的解数为

$$N=\begin{cases}p+(p-1)\left(\dfrac{-ab}{p}\right), & p\mid c,\\ p-\left(\dfrac{-ab}{p}\right), & p\nmid c.\end{cases}$$

解答.

因为 $p\nmid ab$, 故 $p\nmid a$, $p\nmid b$, 进而 $(p,a)=(p,b)=1$, 因此 a, b 模 p 皆有逆, 那么

$$ax^2+by^2\equiv c\pmod p\Leftrightarrow x^2\equiv -ba^{-1}\left(y^2-cb^{-1}\right)\pmod p$$

结合上题结论知该方程解数为

$$N=\sum_{y=0}^{p-1}1+\left(\frac{-ba^{-1}\left(y^2-cb^{-1}\right)}{p}\right)=p+\left(\frac{-ab}{p}\right)\sum_{y=0}^{p-1}\left(\frac{y^2-cb^{-1}}{p}\right)=\begin{cases}p+(p-1)\left(\frac{-ab}{p}\right), & p\mid c\\ p-\left(\frac{-ab}{p}\right), & p\nmid c\end{cases}$$

5　不定方程

5.1　不定方程与同余方程

1.　求下列方程的全部整数解:
(1) $2x^2-5y^2=7$;　(2) $x^2-2xy^2+5z^3+3=0$;　(3) $y^2=41x^3+3$;　(4) $x^2-xy+y^2-x-y=0$;
(5) $y^2=x^3-6$;　(6) $y^2=x^3-x$.

解答.

(1) **法 1.** 方程两边模 2 知 $y^2\equiv 1\pmod 2$, 于是 $y=2s+1$, 代入得

$$2x^2-5\left(2s+1\right)^2=7\Rightarrow x^2=10s^2+10s+6\Rightarrow x^2\equiv 0\pmod 2$$

于是 $x=2t$, 于是

$$4t^2=10s^2+10s+6\Rightarrow 2t^2-5k\left(k+1\right)=3$$

由于 k, $k+1$ 奇偶性不同, 于是 $2\mid k\left(k+1\right)$, 进而在上式两边模 2 可得 $0\equiv 1\pmod 2$, 矛盾! 于是该不定方程无解

法 2. 方程两边模 7 知

$$2x^2+2y^2\equiv 0\pmod 7\Rightarrow x^2+y^2\equiv 0\pmod 7$$

因为 7 的二次剩余仅有三个 1, 2, 4, 所以 $x^2+y^2\not\equiv 0\pmod 7$, 所以该不定方程无解

(2)方程两边模 5 得

$$x^2-2xy^2+3\equiv 0\pmod 5\Leftrightarrow y^2\equiv\frac{x^2+3}{2x}\pmod 5\Leftrightarrow y^2\equiv 3x+4x^{-1}\pmod 5$$

只需依次验证 $x\equiv 1,2,3,4,5\pmod 5$ 的情况, 都有 $\left(\frac{3x+4x^{-1}}{5}\right)=-1$, 于是该方程无解

(3) 两边模 41 得

$$y^2\equiv 3\pmod{41}$$

而 $\left(\frac{3}{41}\right)=\left(\frac{41}{3}\right)=\left(\frac{2}{3}\right)=-1$, 因此方程无解

(4) 将方程配方为

$$\left(x+y-2\right)^2+3\left(x-y\right)^2=4$$

根据整数的性质有

$$\begin{cases}|x+y-2|=2\\|x-y|=0\end{cases} \quad 或 \quad \begin{cases}|x+y-2|=1\\|x-y|=1\end{cases}$$

解得

$$(x,y)\sim(2,2),(0,0),(2,1),(1,0)$$

(5) 若 x 是偶数, 那么两边模 8 得 $y^2\equiv 2 \pmod 8$, 但是 2 并不是 8 的二次剩余, 于是 x 为奇数, 那么 y 也为奇数, 进而 $x^3=y^2+6\equiv 7 \pmod 8$, 同时对所有的奇数 x 有 $x^3\equiv x \pmod 8$, 故 $x\equiv 7 \pmod 8$. 将方程重写为

$$y^2-2=(x-2)\left(x^2+2x+4\right)$$

其中 $x^2+2x+4\equiv 7^2+2\times 7+4\equiv 3 \pmod 8$, 且 $x^2+2x+4=(x+1)^2+3\geq 3$, 于是 x^2+2x+4 必有素因子 $p\equiv \pm 3 \pmod 8$, 于是

$$y^2\equiv 2 \pmod p$$

而对于素数 $p\equiv\pm 3 \pmod 8$, $\left(\dfrac{2}{p}\right)=-1$, 于是该方程无解

(6) 由题 $x^3-x=(x-1)x(x+1)$ 是完全平方数, 若 $x\geq 2$, 那么 $x-1$, x, $x+1$ 三个连续的自然数中有且仅有一个被 3 整除, 于是 $(x-1)x(x+1)$ 的标准分解中 3 的幂次为 1, 进而 $(x-1)x(x+1)$ 不为完全平方数; 对于 $x\leq -2$, $x^3-x<0$, 而 $y^2>0$, 故方程也无解; 当 $x=-1,0,1$ 时, $x^3-x=0$, 于是 $y=0$. 综上方程有整数解为 $(x,y)=(-1,0)$, $(0,0)$, $(1,0)$

题目1的注记.

[1] 对于不定方程 $y^2=x^3+k$, $k\in\mathbb{Z}$, Mordell 于 1920 年得出此类方程仅有有限多整数解, 参考文献: L. J. Mordell, A Statement by Fermat, Proceedings of the London Math. Soc. 18 (1920), v-vi, 以及 EXAMPLES OF MORDELL’S EQUATION.

5.2 费马方程

1. 求所有正整数 m, n, 使 2^m+3^n 是完全平方.

解答.

设 $2^m+3^n=x^2$, 两边模 3 得 $(-1)^m\equiv x^2 \pmod 3$, 而 -1 不是 3 的二次剩余, 于是 m 为偶数, 于是在方程两边模 4 得 $(-1)^n\equiv x^2 \pmod 4$, -1 不是 4 的二次剩余, 于是 n 也为偶数. 设 $m=2s$, $n=2t$, 于是

$$\left(2^s\right)^2+\left(3^t\right)^2=x^2$$

进而可设 $(2^s,3^t)=(2ab,a^2-b^2)$, 其中 $a>b$ 互质且一奇一偶. 因为 $2^s=2ab$, 于是可设 $a=2^p$, $a=2^q$, 由于 a, b 一奇一偶, 那么 $q=0$, 即 $b=1$, 进而 $3^t=2^{2p}-1=(2^p-1)(2^p+1)$, 若 $p>1$,

又 2^p-1 与 2^p+1 相差 2, 于是两数不能同时被 3 整除, 于是 $p=1$, 即 $a=2$. 综上满足条件的正整数有 $(m,n)=(4,2)$

2. 求不定方程 $3^x+4^y=5^z$ 的所有正整数解.

解答.

方程两边模 3 得 $2^z\equiv 1 \pmod 3$, 于是 z 为偶数; 方程两边模 4 得 $(-1)^x\equiv 1 \pmod 4$, 于是 x 为偶数. 令 $x=2r$, $z=2s$, 于是

$$(3^r)^2+(2^y)^2=(5^s)^2$$

进而可设 $(3^r,2^y,5^s)=(m^2-n^2,2mn,m^2+n^2)$, 其中 $m>n$ 互质且一奇一偶, 从而 $n=1$, $m=2^p$. 那么 $3^r=2^{2p}-1=(2^p+1)(2^p-1)$, 若 $p\geq 2$, 又 2^p-1 与 2^p+1 相差 2, 于是两数不能同时被 3 整除, 从而 $p=1$, 故 $(m,n)=(2,1)$, 进而该方程的所有正整数解 $(x,y,z)=(2,2,2)$

3. 证明: 三边长为有理数的等腰三角形的面积不能是 1.

解答.

假设满足条件的等腰三角形存在, 设其边长为 $\frac{a}{c}$, $\frac{a}{c}$, $\frac{b}{c}$, 于是该三角形面积为

$$\frac{b}{c}\sqrt{\left(\frac{a}{c}\right)^2-\left(\frac{b}{2c}\right)^2}=1\Leftrightarrow b^4+4c^4=(2ab)^2$$

由题 **4.** 知该方程没有正整数解, 因此这样的等腰三角形不存在

4. 证明: $x^4+4y^4=z^2$ 没有正整数解.

解答.

原方程即 $(x^2)^2+(2y^2)^2=z^2$, 若方程有解, 取 (x,y,z) 是所有解中使得 z 最小的一组解. 于是可设 $(x^2,2y^2,z)=(m^2-n^2,2mn,m^2+n^2)$, 其中 $m>n$ 互质且一奇一偶. 于是 $y^2=mn$, 且 m, n 一奇一偶, 那么 m, n 均为平方数, 设 $m=p^2$, $n=q^2$, 那么 $x^2+q^4=p^4$, 其中 $(p,q)=1$, 进而 $(p,q,x)=1$, 这说明 (x,q^2,p^2) 是二次费马方程的一组本原正整数解, 由 x 为奇数, 可推得 q 为偶数, p 为奇数, 进而可设 $(x,q^2,p^2)=(r^2-s^2,2rs,r^2+s^2)$, 其中 $r>s$ 互质且一奇一偶, 不妨设 r 为偶数, 进而又有 $r=(2\alpha)^2=4\alpha^2$, $s=\beta^2$, 于是

$$4\alpha^4+\beta^4=p^2$$

这说明 (α,β,p) 也是 $x^4+4y^4=z^2$ 的一组解, 且 $p=\sqrt{r^2+s^2}<z=4r^2s^2+(r^2+s^2)^2$, 但是这与 z 的最小性矛盾!

5. 证明: $x^4 + y^2 = z^4$ 没有正整数解.

解答.
在正整数范围内

$$x^4 + y^2 = z^4 \Leftrightarrow y^4 = \left(z^4 - x^4\right)^2 \Leftrightarrow y^4 + 4\left(xz\right)^4 = \left(x^4 + z^4\right)^2$$

于是由上题结论知该方程无解

6. 证明: 1 不是同余数, 即不存在面积为 1, 三边长为有理数的直角三角形.

解答.
假设满足条件的直角三角形存在, 令其三边长为 $\frac{a}{d}$, $\frac{b}{d}$, $\frac{c}{d}$, 其中 $(a, b, c) = 1$, 那么

$$\begin{cases} a^2 + b^2 = c^2 \\ ab = 2d^2 \end{cases} \Rightarrow a^4 + 4d^4 = c^2$$

由 **4.** 题结论知该方程无解, 进而这样的直角三角形不存在

5.3 二平方和

1. 证明: 形如 $4^a\left(8k+7\right)$ 的正整数不能表为三个整数的平方和.

解答.
8 的二次剩余有 0, 1, 4, 那么三个平方数模 8 同余 0, 1, 2, 3, 4, 5, 6, 而 $a = 0$ 时 $4^a\left(8k+7\right) \equiv 7 \pmod 8$, 于是此时方程无解. $a > 0$ 时, 设 $x^2 + y^2 + z^2 = 4^a\left(8k+7\right)$, 于是 x, y, z 要么全为偶数, 要么 2 奇 1 偶, 若为后者, 有

$$\left(2x_0+1\right)^2 + \left(2y_0+1\right)^2 + \left(2z_0\right)^2 = 4\left(x_0^2 + y_0^2 + z_0^2 + x_0 + y_0\right) + 2 \equiv 2 \pmod 4$$

然而 $4^a\left(8k+7\right) \equiv 0 \pmod 4$, 于是 x, y, z 全为偶数, 那么

$$\left(\frac{x}{2}\right)^2 + \left(\frac{y}{2}\right)^2 + \left(\frac{z}{2}\right)^2 \equiv 4^{a-1}\left(8k+7\right)$$

若 $a - 1 > 0$, 那么可以如上类似处理, 最终可得到

$$x'^2 + y'^2 + z'^2 = 8k + 7$$

其中 x', y', $z' \in \mathbb{Z}$, 两边模 8 可知矛盾!

2. (1) 确定哪些整数可表为两个整数的平方差.

(2) 对任意整数 n, 不定方程

$$x^2+y^2-z^2=n$$

均有无穷多组正整数解.

解答.

(1) 设 $x^2-y^2=n$, 若 n 为奇数, 容易得到一组解为 $(x,y)=\left(\frac{n+1}{2},\frac{n-1}{2}\right)$; 若 n 为偶数, 当 $n\equiv 0 \pmod 4$ 时, 容易得到一组解 $(x,y)=\left(\frac{n}{4}+1,\frac{n}{4}-1\right)$, 当 $n\equiv 2 \pmod 4$ 时, 设 $x^2-y^2=4n_0+2=2\left(2n_0+1\right)$, 即

$$(x+y)(x-y)=2\left(2n_0+1\right)$$

那么 $x+y, x-y$ 中一定有偶数, 但不能全为偶数, 否则 $\frac{(x+y)(x-y)}{2}$ 为偶数, 而 $\frac{(x+y)(x-y)}{2}=2n_0+1$ 为奇数, 矛盾! 因此 $x+y$, $x-y$ 一奇一偶, 不妨设 $x+y\equiv 0 \pmod 2$, $x-y\equiv 1 \pmod 2$, 两式相加得

$$2x\equiv 1 \pmod 2 \Rightarrow 0\equiv 1 \pmod 2$$

矛盾! 因此对于满足 $n\equiv 2 \pmod 4$ 的整数 n, 无法表示为两个整数的平方差, 其余整数都可以

(2) 将方程重写为 $x^2-z^2=n-y^2$, 于是只需证明 $\forall n\in\mathbb{Z}$, 存在无穷多个 y 使得 $n-y^2\not\equiv 2 \pmod 4$, 由 4 的二次剩余仅有 0, 1 知结论成立

3. 证明: 对任意给定的 $n\geq 1$, 均存在连续 n 个正整数, 其中每个都不是两个整数的平方和.

解答.

因为形如 $4n+3$ 的素数有无穷多个, 因此对于任意正整数 n, 可取 n 个不同的素数 $p_i\equiv 3 \pmod 4$, 考虑同余方程组

$$\begin{cases} N\equiv p_1-1 \pmod{p_1^2} \\ N\equiv p_2-2 \pmod{p_2^2} \\ \vdots \\ N\equiv p_n-n \pmod{p_n^2} \end{cases}$$

那么对于 $i=1,2,\cdots,n$, $N+i$ 形如 $4k+3$ 的素因子的重数不为偶数, 于是 $N+i$ 不能表示为二平方和, 也就是说 $N+1, N+2,\cdots,N+n$ 就是所求的 n 个连续的正整数

4. 设 $p\equiv 1\pmod 4$, g 是模 p 的一个原根, $\mathrm{i}=\sqrt{-1}$, 对于每个整数 x, 定义

$$\mathcal{X}(x)=\begin{cases}\mathrm{i}^{\mathrm{ind}_g x}, & p\nmid x,\\ 0, & p\mid x.\end{cases}$$

$$J=\sum_{x=0}^{p-1}\mathcal{X}(x)\mathcal{X}(1-x),$$

证明: $J=A+B\mathrm{i}$, A, $B\in\mathbb{Z}$, 并且 $A^2+B^2=p$.

解答.

先证明三个引理

引理 1 $\forall x, y\in\mathbb{Z}$, $\mathcal{X}(x)\mathcal{X}(y)=\mathcal{X}(xy)$.

证明. x, y 中至少有一个被 p 整除的情况是显然的, 下设 x, y 都不被 p 整除, 那么

$$\mathcal{X}(x)\mathcal{X}(y)=\mathcal{X}(xy)\Leftarrow \mathrm{ind}_g x\cdot\mathrm{ind}_g y\equiv\mathrm{ind}_g(xy)\pmod 4$$

因为 $p\equiv 1\pmod 4$, 设 $p=4k+1$, 那么

$$\mathrm{ind}_g x\cdot\mathrm{ind}_g x\equiv\mathrm{ind}_g(xy)\pmod{\varphi(p)}$$

即

$$\mathrm{ind}_g x\cdot\mathrm{ind}_g x\equiv\mathrm{ind}_g(xy)\pmod{4k}$$

进而

$$\mathrm{ind}_g x\cdot\mathrm{ind}_g x\equiv\mathrm{ind}_g(xy)\pmod 4$$

□

引理 2 $\overline{\mathcal{X}(x)}=\mathcal{X}(x^{-1})$.

证明. 熟知 $\mathrm{ind}_g(x^{-1})=p-1-\mathrm{ind}_g x$, 又 $p\equiv 1\pmod 4$, 那么

$$\overline{\mathcal{X}(x)}=\overline{\mathrm{i}^{\mathrm{ind}_g x}}=\bar{\mathrm{i}}^{\mathrm{ind}_g x}=(-\mathrm{i})^{\mathrm{ind}_g x}=\mathrm{i}^{p-1-\mathrm{ind}_g x}=\mathcal{X}\left(x^{-1}\right)$$

□

引理 3 $\sum_{x=0}^{p-1}\mathcal{X}(x)=\sum_{x=0}^{p-1}\mathcal{X}^2(x)=0$.

证明. 设 $p=4k+1$, 因为 $\{0,1,\cdots,p-1\}=\{0,1,g,g^2,\cdots,g^{p-2}\}$, 于是

$$\sum_{x=0}^{p-1}\mathcal{X}(x)=0+\sum_{s=0}^{4k-1}\mathcal{X}(g^s)=\sum_{s=0}^{4k-1}\mathrm{i}^s=0$$

$$\sum_{x=0}^{p-1}\mathcal{X}^2(x)=0+\sum_{s=0}^{4k-1}\mathcal{X}^2(g^s)=\sum_{s=0}^{4k-1}(-1)^s=0$$

□

由引理可得

$$\begin{aligned}
A^2+B^2=J\overline{J}&=\sum_{x=2}^{p-1}\mathcal{X}(x)\mathcal{X}(1-x)\overline{\sum_{x=2}^{p-1}\mathcal{X}(x)\mathcal{X}(1-x)}\\
&=\sum_{x=2}^{p-1}\mathcal{X}(x)\mathcal{X}(1-x)\sum_{x=2}^{p-1}\mathcal{X}\left(\frac{1}{x}\right)\mathcal{X}\left(\frac{1}{1-x}\right)\\
&=\sum_{x=2}^{p-1}\sum_{y=2}^{p-1}\mathcal{X}(x)\mathcal{X}(1-x)\mathcal{X}\left(\frac{1}{y}\right)\mathcal{X}\left(\frac{1}{1-y}\right)\\
&=\sum_{n=2}^{p-1}\mathcal{X}(1)+\sum_{x=2}^{p-1}\sum_{\substack{y=2\\y\neq x}}^{p-1}\mathcal{X}\left(\frac{x}{y}\right)\mathcal{X}\left(\frac{1-x}{1-y}\right) \qquad (1)
\end{aligned}$$

令 $z=xy^{-1}$, 固定 y, 那么当 x 遍历集合 $\{x\neq y:x=2,3\cdots,p-1\}$ 时, z 会遍历集合 $\{z\neq y^{-1}:z=2,3,\cdots,p-1\}$ 于是

$$(1)=p-2+\sum_{y=2}^{p-1}\sum_{\substack{z=2\\z\neq y^{-1}}}^{p-1}\mathcal{X}(z)\mathcal{X}\left(\frac{1-yz}{1-y}\right)$$

记 $w=\dfrac{1-yz}{1-y}$, 固定 y, 当 z 遍历 $\{z\neq y^{-1}:z=2,3,\cdots,p-1\}$ 时, w 遍历 $\{w\neq z:w=2,3,\cdots,p-1\}$, 因此

$$\begin{aligned}
(1)&=p-2+\sum_{z=2}^{p-1}\mathcal{X}(z)\sum_{\substack{y=2\\y\neq z^{-1}}}^{p-1}\mathcal{X}\left(\frac{1-yz}{1-y}\right)\\
&=p-2+\sum_{z=2}^{p-1}\mathcal{X}(z)\sum_{\substack{w=2\\w\neq z}}^{p-1}\mathcal{X}(w)\\
&=p-2+\sum_{z=2}^{p-1}\mathcal{X}(z)(-1-\mathcal{X}(z))\\
&=p-2-\sum_{z=2}^{p-1}\mathcal{X}(z)-\sum_{z=2}^{p-1}\mathcal{X}^2(z)\\
&=p
\end{aligned}$$

6 应用

6.1 正交拉丁方

1. 试构造 4 个两两正交的五阶拉丁方.

解答.

$$\begin{bmatrix}0&1&2&3&4\\1&2&3&4&0\\2&3&4&0&1\\3&4&0&1&2\\4&0&1&2&3\end{bmatrix}\begin{bmatrix}0&1&2&3&4\\2&3&4&0&1\\4&0&1&2&3\\1&2&3&4&0\\3&4&0&1&2\end{bmatrix}\begin{bmatrix}0&1&2&3&4\\3&4&0&1&2\\1&2&3&4&0\\4&0&1&2&3\\2&3&4&0&1\end{bmatrix}\begin{bmatrix}0&1&2&3&4\\4&0&1&2&3\\3&4&0&1&2\\2&3&4&0&1\\1&2&3&4&0\end{bmatrix}$$

2. 考虑 $\mathbb{Z}_9=[0,1,2,\cdots,8]$ 上的如下 8 个 9 行 9 列的方阵

$$L^{(k)}=\left(a_{ij}^{(k)}\right)_{1\leq i,j\leq 9}\quad(k=1,2,\cdots,8),$$

其中 $a_{ij}^{(k)}\equiv ik+j\pmod 9$, $a_{ij}^{(k)}\in\mathbb{Z}_9$. 试问: $L^{(k)}\,(1\leq k\leq 8)$ 当中哪些是拉丁方, 哪些是彼此正交的拉丁方.

解答.

方阵 $L^{(k)}$ 的一行显然为 $\mathbb{Z}_9$ 的一个排列; 熟知 $k\mathbb{Z}_9+j$ 仍为 $\mathbb{Z}_9$ 的充要条件为 $(k,9)=1$, 于是 $k=1,\,2,\,4,\,5,\,7,\,8$ 时, $L^{(k)}$ 为拉丁方. 设 $L^{(k_1)}$, $L^{(k_2)}$ 是两个拉丁方, 由

$$\left(a_{ij}^{(k_1)},a_{ij}^{(k_2)}\right)=\left(a_{st}^{(k_1)},a_{st}^{(k_1)}\right)\Leftrightarrow\begin{cases}ik_1+j\equiv sk_1+t\pmod 9\\ ik_2+j\equiv sk_2+t\pmod 9\end{cases}$$

可得 $(i-s)(k_1-k_2)\equiv 0\pmod 9$, 因此当 $(k_1-k_2,9)=1$ 时, 有 $i=s$, 进而 $j=t$, 这说明当 $(k_1-k_2,9)=1$ 时, $L^{(k_1)}$ 与 $L^{(k_2)}$ 是正交的; 当 $(k_1-k_2,9)\neq 1$ 时, 方程有其它解, 因此两个拉丁方不正交. 从而彼此正交的拉丁方组有: $L^{(1)}$ 与 $L^{(2)}$, $L^{(1)}$ 与 $L^{(5)}$, $L^{(1)}$ 与 $L^{(8)}$, $L^{(2)}$ 与 $L^{(4)}$, $L^{(2)}$ 与 $L^{(7)}$, $L^{(4)}$ 与 $L^{(5)}$, $L^{(4)}$ 与 $L^{(8)}$, $L^{(5)}$ 与 $L^{(7)}$, $L^{(7)}$ 与 $L^{(8)}$

6.2 试验设计

1. 设 $X = \{x_1, \cdots, x_v\}$ 为品种集合, 区组 $B_1, \cdots, B_b$ 形成 X 上的参数 (v, k, λ) 的 BIBD. 证明: 这些区组的补集合

$$B'_j = X - B_j = \{x_i : x_i \in X, x_i \notin B_j\} \quad (1 \leq j \leq b)$$

也是一个 BIBD. 试计算这个 BIBD 的参数.

解答.

1° 每个 B'_j 都是一个 $v-k$ 元子集

2° 任取 $x_t \in X$, x_t 恰好出现在 r 个区组 $B_{j_1}, \cdots, B_{j_r}$ 中, 那么由补集的定义, x_t 会恰好出现在剩下集合的补集中, 因此每个品种都恰好在 $b-r$ 个区组中

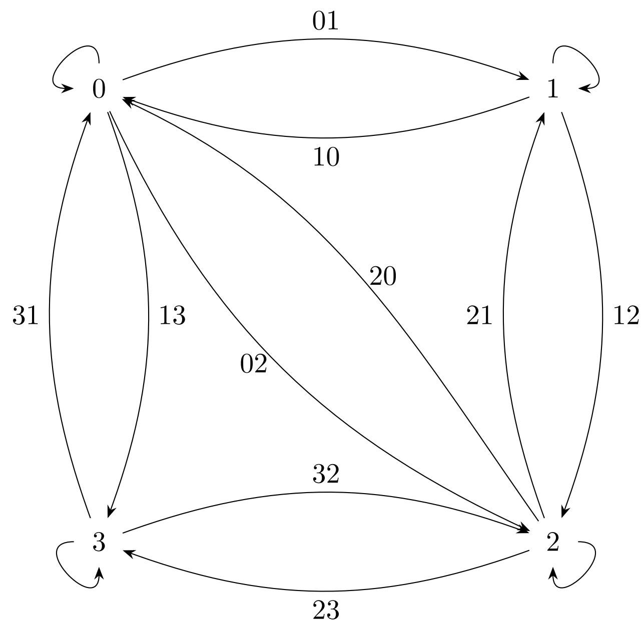
3° 由 2° 类似可知任两个不同的品种均恰好同时出现在 $b-\lambda$ 个区组中

故所求 BIBD 的参数为 $(v-k, b-r, b-\lambda)$

6.3 周游世界、一笔画和密码

1. 用图论方法构造一个 4 元 2 级 M 序列.

解答.



有 4 元 2 级 M 序列

$$0011022033121323$$

2. 列出 $\mathbb{Z}_5[x]$ 中所有常数项为 1 的二次不可约多项式. 其中哪些是本原多项式.

解答.

设 $f(x)$ 是这样的多项式，那么 $f(x) \mid x^{24}-1$, 而

$$x^{24}-1=(x-1)(x+1)\left(x^2+1\right)\left(x^2+x+1\right)\left(x^2-x+1\right)\left(x^4-x^2+1\right)\left(x^4+1\right)\left(x^8-x^4+1\right)$$

于是这样的二次不可约多项式应该在 x^2+1, x^2+x+1, x^2-x+1 三个多项式之中, 经验证符合要求的有 x^2+x+1, x^2-x+1. 又 $x^2+x+1 \mid x^3-1=(x-1)\left(x^2+x+1\right)$, 于是 x^2+x+1 不是本原多项式, $x^2-x+1 \mid x^6-1=(x+1)\left(x^2-x+1\right)\left(x^3-1\right)$, 于是 x^2-x+1 也不是本原多项式

3. 构造一个 5 元 2 级 M 序列.

解答.

要求一个 5 元 2 级的 M 序列, 那么首先要求一个 $\mathbb{Z}_5[x]$ 上的二次本原多项式, 例如 $f(x)=2x^2+x+1$, 那么做除法[1][2]

$$\begin{aligned}\frac{1}{f(x)}=&1-x-x^2+3x^3-x^4-5x^5+7x^6+3x^7-17x^8+11x^9+23x^{10}-45x^{11}-x^{12}+91x^{13}\\&-89x^{14}-93x^{15}+271x^{16}-85x^{17}-457x^{18}+627x^{19}+287x^{20}-1541x^{21}+967x^{22}\\&+2115x^{23}-4049x^{24}-181x^{25}+8279x^{26}-7917x^{27}-8641x^{28}+24475x^{29}-7193x^{30}\\&-41757x^{31}+56143x^{32}+O(x^{33})\end{aligned}$$

取系数模 5 的最小正剩余后并补 0 后就得到一个 5 元 2 级 M 序列

$$144340233130411210322420 0$$

题目3的注记.

[1] 此处除法所得的幂级数即为 $\dfrac{1}{f(x)}$ 的麦克劳林展开; 但实际上, 我们只需要在 $\mathbb{Z}_5$ 上做除法, 因此无需把真正的系数算出来, 根据模的性质做除法计算过程会简单很多.

[2] 该处的幂级数由 WolfarmAlpha 生成.

4. 构造一个 3 元 3 级 M 序列.

解答.

要求一个 3 元 3 级的 M 序列, 那么首先要求一个 $\mathbb{Z}_3[x]$ 上的三次本原多项式, 例如 $f(x)=$

x^3+2x+1，那么做除法

$$\begin{aligned}\frac{1}{f(x)}=&1-2x+4x^2-9x^3+20x^4-44x^5+97x^6-214x^7+472x^8-1041x^9+2296x^{10}-5064x^{11}\\&+11169x^{12}-24634x^{13}+54332x^{14}-119833x^{15}+264300x^{16}-582932x^{17}+1285697x^{18}\\&-2835694x^{19}+6254320x^{20}-13794337x^{21}+30424368x^{22}-67103056x^{23}+148000449x^{24}\\&-326425266x^{25}+719953588x^{26}-1587907625x^{27}+O(x^{28})\end{aligned}$$

取系数模 3 的最小正剩余后并补 0 后就得到一个 3 元 3 级 M 序列

$$11102112101002220122120200011$$

6.4 大数分解和公开密匙

本节无习题.

6.5 离散对数和数字签名

本节无习题.