组合数学第 12 讲

授课时间: 2024 年 11 月 18 日　授课教师: 孙晓明　　记录人: 李驭（助教）　陈子珩（助教）

1　上一讲若干引理的证明

引理 1 (Fermat's little theorem)**.** 假设 a 是一个正整数，p 是一个素数，则有 $a^p \equiv a \pmod p$. 特别的，当 $p \nmid a$ 时，有 $a^{p-1} \equiv 1 \pmod p$.

证明　$p \mid a$ 时，$a^p \equiv a \equiv 0 \pmod p$ 显然成立. $p \nmid a$ 时，$a, 2a, \cdots, (p-1)a$ 两两不同余，所以在模 p 意义下，

$$\{a, 2a, \ldots, (p-1)a\} \equiv \{1, 2, \ldots, p-1\}.$$

将每个集合中的元素相乘, 得

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod p.$$

又因为 $(p-1)!$ 与 p 互素，所以

$$a^{p-1} \equiv 1 \pmod p.$$

□

引理 2. 对于素数域 $\mathbb{Z}_p$ 上的多项式 $P(x)$，方程 $P(x) \equiv 0$ 的不同根的个数不超过 $\deg(P)$.

证明　使用数学归纳法. $\deg(P) = 0, 1$ 时，命题是显然的. 假设 $\deg(P) = k$ 时，命题均成立. $\deg(P) = k+1$ 时, 若 P 没有根, 根数显然不超过 $\deg(P)$; 否则设 x_0 是它的一个根:

$$P(x_0) \equiv 0 \pmod p.$$

存在整系数多项式 $Q(x)$, 满足:

$$P(x) = (x - x_0)Q(x) + r, \quad \deg Q = \deg P - 1 = k.$$

将 $x = x_0$ 带入，得

$$0 \equiv P(x_0) = (x_0 - x_0)Q(x_0) + r = r \pmod p.$$

因此

$$P(x) \equiv (x - x_0)Q(x) \pmod p.$$

从而

$$P(x) \equiv 0 \pmod p \quad \Leftrightarrow \quad p|(x - x_0)Q(x) \quad \Leftrightarrow \quad x \equiv x_0 \pmod p \text{或} Q(x) \equiv 0 \pmod p.$$

由归纳假设 $Q(x)$ 在 $\mathbb{Z}_p$ 上至多 k 个不同的根, 因此 $P(x)$ 在 $\mathbb{Z}_p$ 上至多 $k+1$ 个不同的根. □

引理 3.

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & p \equiv \pm 1 \pmod 8, \\ -1, & p \equiv \pm 3 \pmod 8. \end{cases}$$

证明 由 Euler 判别定理，只需考虑 $2^{\frac{p-1}{2}}$ 模 p 的余数. 首先，

$$p-i \equiv (-1)^i i \pmod p \text{，当 } i \text{ 为奇数;}$$

$$i \equiv (-1)^i i \pmod p \text{，当 } i \text{ 为偶数.}$$

取遍 $i = 1, 2, \cdots \frac{p-1}{2}$，得

$$\begin{aligned} p-1 &\equiv (-1)^1 1 \pmod p \\ 2 &\equiv (-1)^2 2 \pmod p \\ &\cdots \end{aligned}$$

上述同余式左边都是偶数，都小于 p，且互不相同，因此它们构成小于 p 的全部偶数. 将上述同余式全部相乘，

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

两边整理得

$$2^{\frac{p-1}{2}}(\frac{p-1}{2})! \equiv (\frac{p-1}{2})!(-1)^{\frac{p^2-1}{8}} \pmod p.$$

由于 $p \nmid (\frac{p-1}{2})!$，可消去该项，

$$2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}} \pmod p.$$

当 $p \equiv \pm 1 \pmod 8$,$(-1)^{\frac{p^2-1}{8}} \equiv 1 \pmod p$，当 $p \equiv \pm 3 \pmod 8$，$(-1)^{\frac{p^2-1}{8}} \equiv -1 \pmod p$.

综上, 命题得证. □

2 二次互反律

引理 4 (Gauss 引理)**.** p 为奇素数，a 为奇数且与 p 互素，则有

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}} \lfloor \frac{ak}{p} \rfloor}.$$

证明 仿照上一个证明:

$$a^{\frac{p-1}{2}} \cdot \left(\frac{p-1}{2}\right)! \equiv \prod_{k=1}^{\frac{p-1}{2}} (ka) = \prod_{k \in A} (ka) \prod_{k \in B} (ka) \pmod p.$$

其中

$$\begin{aligned} A &:= \left\{ k \middle| 1 \le k \le \frac{p-1}{2}, ka \bmod p < \frac{p}{2} \right\}, \\ B &:= \left\{ k \middle| 1 \le k \le \frac{p-1}{2}, ka \bmod p > \frac{p}{2} \right\}. \end{aligned}$$

则在模 p 意义下，

$$ka = p\frac{ka}{p} \equiv p\left\{\frac{ka}{p}\right\} \begin{cases} < \frac{p}{2}, & k \in A, \\ > \frac{p}{2}, & k \in B. \end{cases} \tag{1}$$

因此

$$a^{\frac{p-1}{2}} \cdot \left(\frac{p-1}{2}\right)! \equiv \prod_{k\in A}(ka)\prod_{k\in B}(-(p-ka)) = (-1)^{|B|}\cdot\left(\frac{p-1}{2}\right)! \pmod p.$$

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \equiv (-1)^{|B|} \pmod p.$$

下面只需计算集合 B 大小的奇偶性. 考虑

$$\begin{aligned}
\sum_{k=1}^{\frac{p-1}{2}} p\left\{\frac{ka}{p}\right\} &= \sum_{k\in A} p\left\{\frac{ka}{p}\right\} + \sum_{k\in B}\left(p-\left(p-p\left\{\frac{ka}{p}\right\}\right)\right)\\
&= \sum_{k\in A} p\left\{\frac{ka}{p}\right\} + p|B| - \sum_{k\in B}\left(p-p\left\{\frac{ka}{p}\right\}\right)\\
&\equiv \sum_{k\in A} p\left\{\frac{ka}{p}\right\} + p|B| + \sum_{k\in B}\left(p-p\left\{\frac{ka}{p}\right\}\right) \pmod 2\\
&\equiv \sum_{k=1}^{\frac{p-1}{2}} k + p|B| \pmod 2\\
&\equiv \sum_{k=1}^{\frac{p-1}{2}} k + |B| \pmod 2.
\end{aligned}$$

其中第 4 个等式是因为式 (1).

另一方面

$$\sum_{k=1}^{\frac{p-1}{2}} p\left\{\frac{ka}{p}\right\} = \sum_{k=1}^{\frac{p-1}{2}}\left(ka - p\left\lfloor\frac{ka}{p}\right\rfloor\right).$$

因为 a, p 均为奇数，所以 $(a-1)\equiv 0 \pmod 2, -p\equiv 1 \pmod 2$，进而

$$|B| \equiv (a-1)\sum_{k=1}^{\frac{p-1}{2}} k - p\sum_{k=1}^{\frac{p-1}{2}}\left\lfloor\frac{ka}{p}\right\rfloor \equiv \sum_{k=1}^{\frac{p-1}{2}}\left\lfloor\frac{ka}{p}\right\rfloor \pmod 2.$$

$$\left(\frac{a}{p}\right) = (-1)^{|B|} = (-1)^{\sum_{k=1}^{\frac{p-1}{2}}\left\lfloor\frac{ka}{p}\right\rfloor}.$$

□

定理 5 (Gauss 二次互反律)**.** *若 p 与 q 都是奇素数，则* $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$.

证明 由高斯引理，有

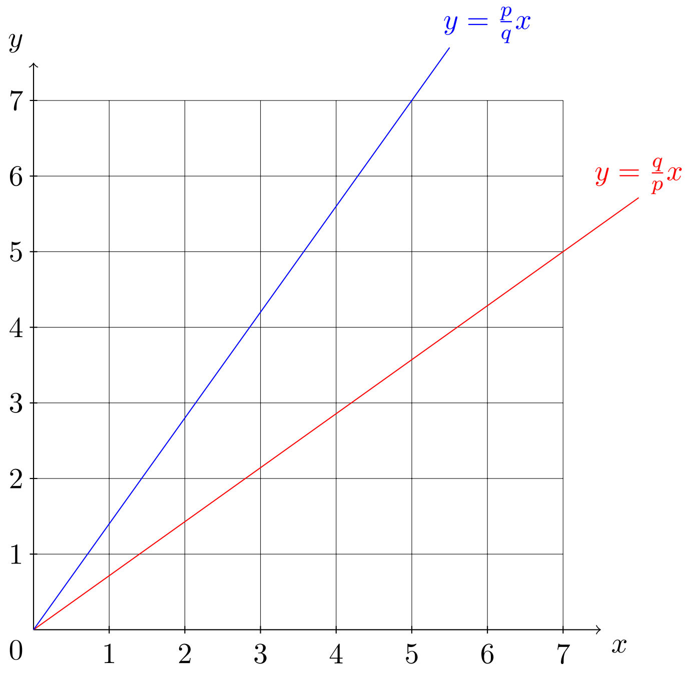
$$\left(\frac{q}{p}\right) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}}\lfloor\frac{qk}{p}\rfloor};$$

$$\left(\frac{p}{q}\right) = (-1)^{\sum_{k=1}^{\frac{q-1}{2}}\lfloor\frac{pk}{q}\rfloor}.$$

所以

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}}\lfloor\frac{qk}{p}\rfloor+\sum_{k=1}^{\frac{q-1}{2}}\lfloor\frac{pk}{q}\rfloor}.$$

在平面直角坐标系中，$\sum_{k=1}^{\frac{p-1}{2}}\lfloor\frac{qk}{p}\rfloor$ 表示被 $y=\frac{q}{p}x, x=\frac{p-1}{2}$ 和 x 轴围成的区域中的整点的数量（坐标轴上的整点不在考虑范围之内）；$\sum_{k=1}^{\frac{q-1}{2}}\lfloor\frac{pk}{q}\rfloor$ 表示被 $y=\frac{p}{q}x, x=\frac{q-1}{2}$ 和 x 轴围成的区域中的整点的数量（坐标轴上的整点不在考虑范围之内）．因为 $y=\frac{q}{p}x$ 与 $y=\frac{p}{q}x$ 关于 $y=x$ 对称，所以 $y=\frac{q}{p}x$ 及其下方，x 轴上方，$x=\frac{p-1}{2}$ 及其左方所围区域内的整点个数与 $y=\frac{p}{q}x$ 及其下方，x 轴上方，$x=\frac{q-1}{2}$ 及其左方所围区域内的整点个数之和, 就等于 $x=0, x=\frac{p-1}{2}, y=0, y=\frac{q-1}{2}$ 所围成的矩形内的正整点（坐标轴上的整点不在考虑范围之内）．所以



$$\sum_{k=1}^{\frac{p-1}{2}}\lfloor\frac{qk}{p}\rfloor+\sum_{k=1}^{\frac{q-1}{2}}\lfloor\frac{pk}{q}\rfloor=\frac{p-1}{2}\times\frac{q-1}{2}.$$

即

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{(p-1)(q-1)}{4}}.$$

$\square$

例 1　求 $\left(\frac{2024}{101}\right)$.

解　对 2024 质因数分解：$2024=2^3\times 11\times 23$.

$$\left(\frac{2024}{101}\right)=\left(\frac{2}{101}\right)^3\left(\frac{11}{101}\right)\left(\frac{23}{101}\right).$$

因为 $101\equiv -3 \pmod 8$，且

$$\left(\frac{11}{101}\right)\left(\frac{101}{11}\right)=(-1)^{\frac{100\times 10}{4}}=1,$$
$$\left(\frac{23}{101}\right)\left(\frac{101}{23}\right)=(-1)^{\frac{100\times 22}{4}}=1,$$

所以

$$\begin{aligned}\left(\frac{2024}{101}\right) &= \left(\frac{2}{101}\right)^3\left(\frac{11}{101}\right)\left(\frac{23}{101}\right)\\ &= (-1)^3\left(\frac{101}{11}\right)\left(\frac{101}{23}\right)\\ &= (-1)\left(\frac{2}{11}\right)\left(\frac{9}{23}\right)\\ &= (-1)\cdot(-1)\cdot 1\\ &= 1.\end{aligned}$$