第 21 次习题课

定理 1 (中国剩余定理)**.** 设 $I_1, \ldots, I_r$ 是交换环 R 的理想，且满足 $\forall i \neq j$，$I_i + I_j = R$。令 $I = I_1 \cap \cdots \cap I_r$。则映射

$$\varphi : R/I \to R/I_1 \times \cdots \times R/I_r, \quad a + I \mapsto (a + I_1, \ldots, a + I_r)$$

是环同构。

证明. 知 $R = (I_1 + I_2)(I_1 + I_3) \cdots (I_1 + I_r) \subseteq I_1 + I_2 I_3 \cdots I_r \subseteq I_1 + \bigcap_{j \neq 1} I_j \subseteq R$。所以有，$R = I_1 + \bigcap_{j \neq 1} I_j$。同理，对任意的 $1 \leq k \leq r$，有 $R = I_k + \bigcap_{j \neq k} I_j$。
考虑环同态 $\widetilde{\varphi} : R \to R/I_1 \times \cdots \times R/I_r$，$a \mapsto (a + I_1, \ldots, a + I_r)$。我们来证这是一个满同态。只需对每个 $k \in \{1, \ldots, r\}$，找到 $x_k \in R$ 使得

$$\widetilde{\varphi}(x_k) = (x_k + I_1, \ldots, x_k + I_k, \ldots, x_k + I_r) = (0 + I_1, \ldots, 1 + I_k, \ldots, 0 + I_r). \qquad (*)$$

也即需寻找 x_k 使得 $1 - x_k \in I_k$ 且 $x_k \in \cap_{j \neq k} I_j$。
由 $1 \in R = I_k + \bigcap_{j \neq k} I_j$ 知，存在 $b_k \in I_k$ 及 $x_k \in \bigcap_{j \neq k} I_j$ 使得 $1 = b_k + x_k$。由于这个 x_k 满足 $1 - x_k \in I_k$ 且 $x_k \in \cap_{j \neq k} I_j$。从而 $(*)$ 式成立。
对任意的 $(a_1 + I_1, \ldots, a_r + I_r) \in R/I_1 \times \cdots \times R/I_r$，取 $x = a_1 x_1 + \ldots + a_r x_r$，则有

$$\widetilde{\varphi}(x) = \widetilde{\varphi}(a_1)\widetilde{\varphi}(x_1) + \ldots + \widetilde{\varphi}(a_r)\widetilde{\varphi}(x_r) = (a_1 + I_1, \ldots, a_r + I_r).$$

所以 $\widetilde{\varphi}$ 是满同态。易验证 $\ker(\widetilde{\varphi}) = I_1 \cap \cdots \cap I_r = I$。所以，$\varphi : R/I \to R/I_1 \times \cdots \times R/I_r$ 是环同构。 □

推论 1 ($\mathbb{Z}$ 上中国剩余定理)**.** 设 $n_1, \ldots, n_r \in \mathbb{Z}_{\geq 2}$ 两两互素，令 $n = n_1 \cdots n_r$。则有环同构

$$\varphi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_r\mathbb{Z}, \ \ a + n\mathbb{Z} \mapsto (a + n_1\mathbb{Z}, \ldots, a + n_r\mathbb{Z}).$$

注. (1) 由 n_i 与 n_j 互素及 $n = n_1 \cdots n_r$ 知，$n_i\mathbb{Z} + n_j\mathbb{Z} = \mathbb{Z}$，$n\mathbb{Z} = n_1\mathbb{Z} \cap \cdots \cap n_r\mathbb{Z}$。
(2) 令 $N_k = n/n_k$，可知 $N_k\mathbb{Z} = \cap_{j \neq k}(n_j\mathbb{Z})$. 由 $(n_k, N_k) = 1$ 知 $n_k\mathbb{Z} + N_k\mathbb{Z} = \mathbb{Z}$。根据剩余定理的证明，关键是把 $\mathbb{Z}$ 中的 1 分解成 $1 = b_k + x_k$, 其中 $b_k \in n_k\mathbb{Z}, x_k \in N_k\mathbb{Z}$。
(3) 为给出 x_k 的具体取值，可先解同余方程 $N_k t_k \equiv 1 \pmod{n_k}$，再取 $x_k = N_k t_k$ 即可。

题 1. 求解同余方程组。

$$(1) \begin{cases} m \equiv 1 \pmod 2 \\ m \equiv 2 \pmod 3 \\ m \equiv 3 \pmod 5 \end{cases} \qquad (2) \begin{cases} m \equiv 2 \pmod 5 \\ m \equiv 3 \pmod 7 \\ m \equiv 1 \pmod 2 \end{cases}$$

解. (1) 记 $n_1 = 2, n_2 = 3, n_3 = 5,\ n = n_1 n_2 n_3 = 30$。令

$$N_1 = n/n_1 = 15, N_2 = n/n_2 = 10, N_3 = n/n_3 = 6.$$

求解 N_i 在 $\mod n_i$ 意义下的一个乘法逆 t_i:

$$15t_1 \equiv 1 \pmod 2, \quad 10t_2 \equiv 1 \pmod 3, \quad 6t_3 \equiv 1 \pmod 5.$$

可取 $t_1 = t_2 = t_3 = 1$。于是原同余方程的解为

$$m \equiv 1 \cdot N_1 t_1 + 2 \cdot N_2 t_2 + 3 \cdot N_3 t_3 \equiv 53 \equiv 23 \pmod{30}.$$

(2) 记 $n_1 = 5, n_2 = 7, n_3 = 2,\ n = n_1 n_2 n_3 = 70$。令

$$N_1 = \frac{n}{n_1} = 14, \quad N_2 = \frac{n}{n_2} = 10, \quad N_3 = \frac{n}{n_3} = 35.$$

求 t_1, t_2, t_3 使得

$$14t_1 \equiv 1 \pmod 5, \quad 10t_2 \equiv 1 \pmod 7, \quad 35t_3 \equiv 1 \pmod 2.$$

可取 $t_1 = 4, t_2 = 5, t_3 = 1$。于是原同余方程的解为

$$m \equiv 2 \cdot N_1 t_1 + 3 \cdot N_2 t_2 + 1 \cdot N_3 t_3 \equiv 2 \times 14 \times 4 + 3 \times 10 \times 5 + 1 \times 35 \times 1 \equiv 17 \pmod{70}.$$

题 2 (多项式插值)**.** 设 K 是域，$a_1, \ldots, a_n \in K$ 两两不同，$b_1, \ldots, b_n \in K$。则存在唯一次数小于 n 的多项式 $f(x) \in K[x]$ 使得 $f(a_i) = b_i\ (i = 1, \ldots, n)$。

证明. 考虑理想 $I_i = (x - a_i)$，由于 a_i 取值不同，有 $I_i + I_j = K[x]$。由中国剩余定理知

$$K[x]/\bigcap I_i \cong K[x]/I_1 \times \cdots \times K[x]/I_n.$$

但 $\bigcap I_i = \prod (x - a_i)$，且 $K[x]/I_i \cong K$。给定 $(b_1, \ldots, b_n) \in K^n$，存在唯一 $f \in K[x]$ 模 $\prod (x - a_i)$ 使得 $f \equiv b_i \pmod{(x - a_i)}$，即 $f(a_i) = b_i$。 □

定义 1. Euler 函数 $\varphi : \mathbb{Z}_{\geq 1} \to \mathbb{Z}_{\geq 1},\ n \mapsto \varphi(n) := |(\mathbb{Z}/n\mathbb{Z})^\times|$，知 $\varphi(n)$ 是 1 到 n 中与 n 互素的整数的个数。

题 3. 设 $a \in \mathbb{Z},\ n \in \mathbb{Z}_{\geq 1}$。若 $(a, n) = 1$，则 $a^{\varphi(n)} \equiv 1 \pmod n$。

证明. 令 $G = (\mathbb{Z}/n\mathbb{Z})^\times$，知 $\varphi(n) = |G|$。只需说明 $a \in \mathbb{Z}$ 模 n 的同余类落在群 G 中即可。 □

题 4. 设 $\varphi : \mathbb{Z}_{\geq 1} \to \mathbb{Z}_{\geq 1}$ 是欧拉函数，p 是一个素数。证明:

(1) $\varphi(p^n) = p^n - p^{n-1},\ \forall n \geq 1$。

(2) 若 $m, n \in \mathbb{Z}_{\geq 1}$ 互素，则 $\varphi(mn) = \varphi(m) \times \varphi(n)$。

(3) 设 $f(m)=\sum_{d|m,d>0}\varphi(d)$, $m\in\mathbb{Z}_{\geq 1}$。证明: $f(m)=m$。

证明. (1) 在 $1,2,\ldots,p^n$ 中，p 的倍数有:

$$p,2p,3p,\ldots,p^n$$

总共有 p^{n-1} 个。因此，与 p^n 互素的数的个数为:

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

(2) 由中国剩余定理，有环同构 $\mathbb{Z}/mn\mathbb{Z}\cong\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$ 及群同构 $(\mathbb{Z}/mn\mathbb{Z})^\times\cong(\mathbb{Z}/m\mathbb{Z})^\times\times(\mathbb{Z}/n\mathbb{Z})^\times$。从而 $\varphi(mn)=\varphi(m)\varphi(n)$。
(3) 若 m 为素数的方幂, 不妨设 $m=p^n$, 则有 $f(m)=f(p^n)=\varphi(1)+\varphi(p)+\ldots+\varphi(p^n)=1+(p-1)+\ldots+(p^n-p^{n-1})=p^n=m$。此时结论成立。根据质因数分解定理及 (2) 中结论，要证结论 (3) 成立，只需再证: 若 $m,n\in\mathbb{Z}_{\geq 1}$ 互素，则 $f(m)\times f(n)=f(mn)$。
设 $m,n\in\mathbb{Z}_{\geq 1}$ 互素，则

$$f(m)f(n)=\sum_{i|m}\varphi(i)\sum_{j|n}\varphi(j)=\sum_{i|m}\sum_{j|n}\varphi(i)\varphi(j)=\sum_{i|m}\sum_{j|n}\varphi(i\times j)=\sum_{d|mn}\varphi(d)=f(mn).$$

注意: $(m,n)=1\Rightarrow(i,j)=1\Rightarrow\varphi(i)\varphi(j)=\varphi(i\times j)$。 □

定义 2. 一个整环 R 被称为一个 **Euclide 环**，如果存在一个映射 $\nu:R\backslash\{0\}\to\mathbb{N}$ 满足

(i) $\forall a\in R,\ b\in R\setminus\{0\},\exists q,r\in R$ 使 $a=bq+r$，且若 $r\neq 0$，则 $\nu(r)<\nu(b)$。

(ii) $\forall a,b\in R\setminus\{0\}$，有 $\nu(b)\leq\nu(ab)$。

注. 可证明 Euclide 整环都是主理想整环，e.g., $\mathbb{Z}$, $\mathbb{R}[x]$。

题 5 (高斯整环). 设 $\mathbb{Z}[i]=\{a_1+ia_2\mid a_1,a_2\in\mathbb{Z}\}$, $i^2=-1$。定义 $\nu:\mathbb{Z}[i]\setminus\{0\}\to\mathbb{N}$, $a_1+ia_2\mapsto(a_1^2+a_2^2)$。证明 $(\mathbb{Z}[i],\nu)$ 构成一个 Euclide 环。

证明. 设 $\alpha=a_1+ia_2$，$\beta=b_1+ib_2\in\mathbb{Z}[i]$。易验证:

$$\nu(\alpha\cdot\beta)=\nu(\alpha)\cdot\nu(\beta),\ \text{且若}\ \alpha\neq 0,\text{则}\ \nu(\alpha)\geq 1.$$

从而 ν 满足条件 (ii): $\forall\alpha,\beta\in\mathbb{Z}[i]\setminus\{0\}$，有 $\nu(\beta)\leq\nu(\alpha\beta)$。
仍需证 ν 满足条件 (i)。设 $\alpha=a_1+ia_2\in\mathbb{Z}[i],\beta=b_1+ib_2\in\mathbb{Z}[i]\backslash\{0\}$。

$$\frac{\alpha}{\beta}=\frac{a_1+ia_2}{b_1+ib_2}=t_1+it_2,\text{其中}t_1,t_2\in\mathbb{Q}.$$

取 $d_1,d_2\in\mathbb{Z}$ 使 $|t_1-d_1|\leq\frac{1}{2},|t_2-d_2|\leq\frac{1}{2}$. 令 $q=d_1+id_2\in\mathbb{Z}[i]$,

$$r:=\alpha-\beta\cdot q=\beta\left(\frac{\alpha}{\beta}-q\right)=\beta\left[(t_1-d_1)+i(t_2-d_2)\right]\in\mathbb{Z}[i].$$

知 $\alpha=\beta\cdot q+r$, 并且若 $r\neq 0$, 则

$$\nu(r)=\nu(\beta)\cdot[(t_1-d_1)^2+(t_2-d_2)^2]\leq\nu(\beta)\cdot[1/4+1/4]=\nu(\beta)/2<\nu(\beta).$$

从而条件 (i) 也成立。因此，$(\mathbb{Z}[i],\nu)$ 构成一个 Euclide 环。 □

题 6. 求证：$\mathbb{Q}[x]$ 中的多项式 $f(x) = 1 + x + \frac{x^2}{2!} + \cdots + \frac{x^n}{n!}$ 没有重因式。

证明. 只需验证 $(f(x), f'(x)) = 1$。 □