现考虑小于 n 的所有素数 —— 欧拉定理

欧拉函数：$n \in N^+$，$C_n = \{a \in [n] \mid (a,n)=1\}$

$[n]$ 指模 n 的完全剩余系

C_n 为模 n 的缩系

$\varphi(n)$：$[n]$ 中与 n 互素的整数个数，$|C_n|$

n	1	2	3	4	5	
$\lvert C_n\rvert$	1	2	2	2	4	

欧拉定理：$\forall a$，若 $(a,n)=1$，则 $a^{\varphi(n)} \equiv 1 \mod n$

证：
- 由裴角：$(a,n) = (a+kn, n)$
- 且 $(a+kn)^{\varphi(n)} = a^{\varphi(n)} \mod n$

直接考虑 $a \in C_n$

C_1、C_2、C_3 … 均可先分别验证

取 $C_n = \{r_1, r_2, \cdots r_{\varphi(n)}\}$ 考虑集合 $aC_n = \{ar_i \mid r_i \in C_n\}$

① 有 $(r_i, n)=1$，$(a,n)=1$ $\Rightarrow (ar_i, n)=1$

② 在 aC_n 中：若 $ar_i \equiv ar_j \mod n$ 则 $n \mid a(r_i - r_j) \Rightarrow n \mid r_i - r_j$ 但 $0 < |r_i - r_j| < n$，矛盾.

故 aC_n 中任两个数 $\mod n$ 均不同余

由①、②：aC_n 中元素均与 n 互素且无 $\mod n$ 同余，有得 $aC_n = C_n \mod n$

aC_n 可看作 C_n 中元素，且可建立一一映射

C_n，aC_n 中元素累乘：$r_1 r_2 \cdots r_{\varphi(n)} = a^{\varphi(n)} r_1 r_2 \cdots r_{\varphi(n)} \mod n \Rightarrow a^{\varphi(n)} \equiv 1 \mod n$

$R = r_1 \cdots r_{\varphi(n)}$，$(R, n)=1$

目标：$a^x \equiv 1 \mod n$ 是否有解：

$x=0$ 是一个平凡解，

考虑 $a^1, a^2, \cdots a^n$，

若不存在 $a^i \equiv 1 \mod n$，

则 $\exists i<j$，s.t. $a^i \equiv a^j \mod n$，则由 $(a^k, n)=1 \Rightarrow a^{j-i} \equiv 1 \mod n$

故同余无穷在 $x \in [n]$ 中有解.

继续分析阶的性质：

已有：$a^{x_0} \equiv 1 \mod n$

则 ① $\forall k \in \mathbb{Z}$. $a^{kx_0} \equiv 1 \mod n$

② x_1, x_2 是方程的解. $a^{k_1x_1+k_2x_2} \equiv 1 \mod n$ （若 $k_1x_1+k_2x_2>0$）

$\begin{cases} a^{x_1+x_2} \equiv 1 \mod n \\ a^{x_1} \equiv a^{x_2} \mod n \end{cases} \Rightarrow a^{|x_1-x_1|} \equiv 1 \mod n$

(x_1, x_2)是解！ $\leftrightarrow \{xa+yb \mid x,y \in \mathbb{Z}\} = \{kd \mid k \in \mathbb{Z},\ d=(a,b)\}$

所有的解可表示为某个最小正整数解的倍数

记 r 为 $a^x \equiv 1 \mod n$ 的最小正整数解，目标 $r \mid \varphi(n)$ or ~~$r = \varphi(n)$~~ → 举例否决

$a=3,\ n=20$

$\varphi(n)=8$

但 $3^4 \equiv 1 \mod 20$

若 $r=\varphi(n)$ 则直接得证，不妨设 $r<\varphi(n)$

先取出：$R = \{a^1, a^2, \cdots, a^r \mod n\}$ → 再乘 a 也跑不出去了

循环群

$R \subsetneq C_n$，$\exists b \in C_n \setminus R$ 取 $\{ba, ba^2, \cdots ba^r \mod n\}$

$\begin{cases} (b,n)=1. \text{在 } bR \text{ 中任两个数 } n \text{ 不同余} \\ \text{且 } (ba^i, n)=1 \Rightarrow bR \subsetneq R \\ bR \cap R = \phi : \text{反证：} \exists\ a^i,\ ba^j \ \text{s.t.}\ a^i \equiv ba^j \mod n \end{cases}$

$\Rightarrow \begin{cases} a^{i-j} \equiv b \mod n & i>j \\ a^{i+r-j} \equiv b \mod n & i \le j \end{cases}$

$\Rightarrow R \in R$. 矛盾，故 $bR \cap R = \phi$

若 $bR \cup R = C_n$. 则 $r \mid \varphi(n)$，否则，取 $b_2 \in C_n \setminus (R \cup bR)$

作 b_2R 与 R、bR 同阶且不交

⋮

如此进行，$\exists k$，s.t. $\bigcup_{0 \le i \le k} b_iR = C_n$ 且 $b_iR \cap b_jR = \phi$

故 $r \mid \varphi(n)$

群的陪集分解.

range(1, n-1) → HW2

$\varphi(n)$怎么算： $O(n/\log n)$时间可算 通为十 辗转相除验证，但不够快

1. 若为素： $n=p$， $\varphi(p)=p-1$

$\left(\forall a,\ p\nmid a,\ a^{p-1}\equiv 1 \bmod p\right.$

$\left.\downarrow \forall a,\ a^p\equiv a \bmod p$ 费马小定理，p为素数$\right)$

2. $n=p^k$， $\varphi(p^k)=p^{k-1}(p-1)$ （必需不被p整除，均与p^k互素，p为素）

3. $n=pq$

eg: $n=15=3\times 5$:

	0	1	2	3	4	mod5
0	15	6	12	3	9	
1	10	1	7	13	4	
2	5	11	2	8	14	
mod3						

$2\times 4=\varphi(3)\times\varphi(5)$

此处，可以构造 $\{x\le 15 \mid (x,15)=1\}$ 和 $\{x\le 15 \mid (x,3)=1\}\cup\{x\le 15,\ (x,5)=1\}$ 间的一一映射

4. $n=p_1^{r_1}p_2^{r_2}\cdots p_k^{r_k}$，

$$(a,n)=1 \Leftrightarrow \begin{cases}(a,p_1^{r_1})=1\\ \vdots\\ (a,p_k^{r_k})=1\end{cases} \Leftrightarrow \begin{cases}(a,p_1)=1\\ \vdots\\ (a,p_k)=1\end{cases}$$

设：$\begin{cases}a=x_1 \bmod p_1^{r_1}=m_1\\ a=x_2 \bmod p_2^{r_2}=m_2\\ \vdots\\ a=x_k \bmod p_k^{r_k}=m_k\end{cases}$ $x_1\cdots x_k\neq 0 \Rightarrow$ $p_1\nmid x_1$ 有 $\varphi(p_1^{r_1})$个 x_1

$\vdots$

$p_k\nmid x_k$ 有 $\varphi(p_k^{r_k})$个 x_k

$$\begin{aligned}\varphi(p_1^{r_1}p_2^{r_2}\cdots p_k^{r_k}) &= \varphi(p_1^{r_1})\varphi(p_2^{r_2})\cdots\varphi(p_k^{r_k})\\ &= (p_1-1)p_1^{r_1-1}\cdots(p_k-1)p_k^{r_k-1}\\ &= \left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)\cdot n\end{aligned}$$