习题

热身题

1.

$k=1$	$n=1$	$\{1\}$	
$k=2$	$n=2$	$\{1, 2\}$	$\longrightarrow$ 最小整数
$k=3$	$n=4$	$\{1, 2, 4\}$	
$k=4$	$n=6$	$\{1, 2, 3, 6\}$	
$k=5$	$n=16$	$\{1, 2, 4, 8, 16\}$	
$k=6$	$n=12$	$\{1, 2, 3, 4, 6, 12\}$	

1	$\{1\}$	1	11.	$\{1, 11\}$	2
2	$\{1, 2\}$	2	12	$\{1, 2, 3, 4, 6, 12\}$	6
3	$\{1, 3\}$	2	13	$\{1, 13\}$	2
4	$\{1, 2, 4\}$	3	14	$\{1, 2, 7, 14\}$	4
5	$\{1, 5\}$	2	15	$\{1, 3, 5, 15\}$	4
6	$\{1, 2, 3, 6\}$	4	16	$\{1, 2, 4, 8, 16\}$	5
7	$\{1, 7\}$	2	17	$\{1, 17\}$	2
8	$\{1, 2, 4, 8\}$	4	18	$\{1, 2, 3, 6, 9, 18\}$	6
9	$\{1, 3, 9\}$	3	19	$\{1, 19\}$	2
10	$\{1, 2, 5, 10\}$	4	20	$\{1, 2, 4, 5, 10, 20\}$	6

2. 设 $d=\gcd(m,n)$

$m=m'd \quad n=n'd \quad m'\perp n'$

$\operatorname{lcm}(m,n)=\operatorname{lcm}(m'd,n'd)=d\operatorname{lcm}(m',n')=d\cdot m'n'$

$\therefore \gcd(m,n)\operatorname{lcm}(m,n)=d\cdot dm'n'=m\cdot n$

由 (4.12) (4.14), (4.15) 证

$m=\prod_p p^{m_p}, \quad n=\prod_p p^{n_p}$

$mn=\prod_p p^{m_p+n_p}$

$d=\gcd(m,n) \iff d_p=\min\{m_p,n_p\}$

$l=\operatorname{lcm}(m,n) \iff l_p=\max\{m_p,n_p\}$

$d\cdot l=\gcd(m,n)\cdot\operatorname{lcm}(m,n)=\prod_p p^{d_p+l_p}=\prod_p p^{m_p+n_p}=m\cdot n$

$n \bmod m\neq 0$ 用 $\operatorname{lcm}(n \bmod m, m)$ 表示出 $\operatorname{lcm}(m,n)$

$\gcd(n \bmod m, m)=\gcd(n,m)$ 〈由 Euclid 算法〉

$\gcd(n \bmod m, m)\cdot\operatorname{lcm}(n \bmod m, m)=(n \bmod m)\, m$

$$\operatorname{lcm}(n \bmod m, m)=\frac{(n \bmod m)\, m}{\gcd(n,m)}$$

$$=(n \bmod m)\frac{mn}{\gcd(n,m)}\cdot\frac{1}{n}$$

$$=(n \bmod m)\operatorname{lcm}(n,m)\cdot\frac{1}{n}$$

$$\operatorname{lcm}(n,m)=\frac{n}{n \bmod m}\operatorname{lcm}(n \bmod m, m)$$

3. $\pi(x)$. 不超过 x 的素数个数.

$\pi(x) - \pi(x-1) = [x\text{是素数}]$ 成立 ×

上式仅对 $x \in \mathbb{N}$ 成立 但 $\pi(x)$ 对 $x \in \mathbb{R}$ 都有定义

$\pi(x) - \pi(x-1) = [\lfloor x \rfloor\text{是素数}]$

4. $\left(\frac{0}{1}, \frac{1}{0}, \frac{0}{-1}, \frac{-1}{0}, \frac{0}{1}\right) = (0, +\infty, 0, -\infty, 0)$

$\left(\frac{0}{1}, \frac{1}{1}, \frac{1}{0}, \frac{1}{-1}, \frac{0}{-1}, \frac{-1}{-1}, \frac{-1}{0}, \frac{-1}{1}, \frac{0}{1}\right)$

$\left(\frac{0}{1}, \frac{1}{0}\right)$ 之间仍是之前的 Stern-Brocot 树

有理数的数系 (number system).

每个正的最简分数均出现一次

$\left(\frac{1}{0}, \frac{0}{-1}\right) \to \left(\frac{1}{0}, \frac{1}{-1}, \frac{0}{-1}\right) \to \left(\frac{1}{0}, \frac{2}{-1}, \frac{1}{-1}, \frac{1}{-2}, \frac{0}{-1}\right)$

每个负的最简分数 $\frac{m}{-n}$

$\left(\frac{0}{-1}, \frac{-1}{0}\right) \to \left(\frac{0}{-1}, \frac{-1}{-1}, \frac{-1}{0}\right) \to \left(\frac{0}{-1}, \frac{-1}{-2}, \frac{-1}{-1}, \frac{-2}{-1}, \frac{-1}{0}\right)$

每个正的最简分数 $\frac{-m}{-n}$

$\left(\frac{-1}{0}, \frac{0}{1}\right) \to \left(\frac{-1}{0}, \frac{-1}{1}, \frac{0}{1}\right) \to \left(\frac{-1}{0}, \frac{-2}{1}, \frac{-1}{1}, \frac{-1}{2}, \frac{0}{1}\right)$

每个负的最简分数 $\frac{-m}{n}$

m, n 为所有整数的最简分数集合. (认为 $\frac{-a}{-b}$ 与 $\frac{a}{b}$ 不等价)

Stern-Brocot 环 (wreath) 表示平面所有有理方向

5. $L=\begin{pmatrix}1&1\\0&1\end{pmatrix}$ $R=\begin{pmatrix}1&0\\1&1\end{pmatrix}$

$$L^2=\begin{pmatrix}1&1\\0&1\end{pmatrix}^2=\begin{pmatrix}1&1\\0&1\end{pmatrix}\begin{pmatrix}1&1\\0&1\end{pmatrix}=\begin{pmatrix}1&2\\0&1\end{pmatrix}$$

$$L^k=\begin{pmatrix}1&k\\0&1\end{pmatrix}$$

$$R^2=\begin{pmatrix}1&0\\1&1\end{pmatrix}^2=\begin{pmatrix}1&0\\2&0\end{pmatrix}$$

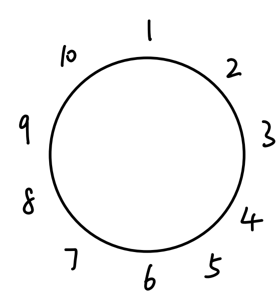
$$R^k=\begin{pmatrix}1&0\\k&1\end{pmatrix}$$

6 $a\equiv b \pmod 0$

$a\equiv b \pmod d$ $\exists q\in\mathbb{N}$ $a=b+qd$

$a\equiv b \pmod 0$ $\exists q\in\mathbb{N}$ $a=b+q\cdot 0=b$

$a=b$

7. 

每隔 $m-1$ 人处死一人

（m 可比10大得多）

$\forall k.$ 石孤 $\underline{10.\quad k.\quad k+1.}$

$m=2$										
	1	2	3	4	5	6	7	8	9	10
	11		12		13		14		15	
	16				17				18	
					19					
					20					

检验1. $J(10)=J((1010)_2)=(11)_2=5$

2. $f(n) = A(n)\alpha + B(n)\beta + C(n)\gamma$

$$\begin{cases} A(n) = 2^m & n = 2^m + l \quad 0 \le l < 2^m \\ B(n) = 2^m - 1 - l \\ C(n) = l \end{cases}$$

$\alpha = 1,\ \beta = -1.\ \gamma = 1$

$10 = 2^3 + 2$

$f(10) = 2^3 \times 1 + (-1) \times 5 + 1 \times 2$

$= 8 - 5 + 2 = 5$

$m = 3$

1 2 3 4 5 6 7 8 9 10
11 12 13 14 15 16 17
18 19 20 21 22
23 24 25
26 27
28
29
30

$\forall m.$

1 2 3 4 5 6 7 8 9 10
11 12 ...
... $10 + m$

$10 + m \equiv 10 \equiv 0 \pmod{10}$ $\quad m = 10x$

ex $m = 10$ $\quad m - 1 = 9$

1 2 3 4 5 6 7 8 9 10
11 12 13 14 15 16 17 18 19
20 21 22 23 24 25 26 27 28
29 30 31 32 33 34 35 36
39 40 41 42 43 44 45 ...

10, 1, 3

$m=20 \quad m-1=19$

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22		...					29	
30	31		...					38	
39	40		...					47	
48	49	50	51	52	53	54	55		
56	57	58	59	60	61	62	63		
64	65	66	67	68					

10, 2, 6

10, 1. 3

10, 2. 6

10, 3. 9

10, 4. $\underline{2}$?

10, 5.

$m \bmod 10 = 0$

$\left.\begin{array}{l} m \bmod 9 = k \\ m \bmod 8 = 1 \end{array}\right\}$ 矛盾

m 不可能 既是奇数又是偶数

8 $\begin{cases} 10x+y \equiv x \pmod 3 \\ 10x+y \equiv y \pmod 5 \end{cases}$ 所有相关解

$13 \sim (1,3)$ $\begin{cases} 13 \equiv 1 \pmod 3 \\ 13 \equiv 3 \pmod 5 \end{cases}$

提示

$\begin{cases} 10u+6v \equiv u \pmod 3 \\ 10u+6v \equiv v \pmod 5 \end{cases}$

$u = 1, 2$

$v = 3, 6, 9$

$10u + v \equiv u \pmod 3$

$5v \equiv 0 \pmod 3$

$10u + v \equiv v \pmod 5$

恒成立

13 16 19

23 26 29

9 $(3^{77}-1)/2$ 奇的合数

提示：$3^{77} \bmod 4 = ?$

$3 \bmod 4 = 3$

$3^2 \bmod 4 = 1$

$3^3 \bmod 4 = 3$

$3^4 \bmod 4 = 1$

...

$3^{77} \bmod 4 = 3$

$3^{77} = 4k+3$

$$\frac{3^{77}-1}{2} = \frac{4k+2}{2} = 2k+1$$

$$\frac{3^{77}-1}{3-1} = 3^{76}+3^{75}+\cdots+1$$

$\frac{3^{77}-1}{2}$ 可被 $\frac{3^7-1}{2}$ 和 $\frac{3^{11}-1}{2}$（及其他数整除）

10，计算 $\varphi(999)$

$9 \,\underline{|\, 999}$
$3 \,\underline{|\, 111}$
37

$$\varphi(999) = 999\left(1-\frac{1}{3}\right)\left(1-\frac{1}{37}\right)$$
$$= 9 \times 2 \times 36$$
$$= 648$$

11.

$$g(n) = \sum_{0 \le k \le n} f(k) \Leftrightarrow f(n) = \sum_{0 \le k \le n} \sigma(k)\, g(n-k)$$

$$\boxed{(4.56) \quad g(m) = \sum_{d \mid m} f(d) \Leftrightarrow f(m) = \sum_{d \mid m} \underline{\mu(d)}\, g\left(\frac{m}{d}\right)}$$

默比乌斯μ函数

12.13

32 推广 (4.47) 证明 Euler 定理 (4.50)

(4.47) 费马小定理 $n^{p-1} \equiv 1 \pmod p$, $n \perp p$

设 p 为素数

$$n \times 2n \times \cdots \times (p-1)n$$

$$\equiv (n \bmod p) \times (2n \bmod p) \times \cdots \times (((p-1)n) \bmod p)$$

$$\equiv (p-1)!$$

$$(p-1)!\, n^{p-1} \equiv (p-1)! \pmod p$$

$\because$ $(p-1)!$ 不能被 p 整除 $\therefore$ 消去 $(p-1)!$ $n^{p-1} \equiv 1 \pmod p$

(4.50) $n^{\varphi(m)} \equiv 1 \pmod m$ $n \perp m$

m 为素数 $\varphi(m) = m-1$. 由 (4.47) 可证

m 不是素数 $\varphi(m)$ 为积性函数 $m = \prod_i p_i$, $\varphi(m) = \prod_i \varphi(p_i)$

?

$$\varphi(12) = \varphi(4)\varphi(3) = \underline{2 \times 2} = 4$$

$$n^2 \equiv 1 \pmod 3$$

$$n^2 \equiv 1 \pmod 4$$

$$n^{\varphi(m)} = \left(n^{\varphi(p_i)}\right)^{\varphi(p_j)\cdots} \equiv 1 \pmod{p_i}$$

$$\equiv 1 \pmod{\textstyle\prod p_i}$$ 独立剩余?

(中国剩余定理)

$x \equiv 1 \pmod 3$

$x \equiv 1 \pmod 4$

$x \equiv 1 \pmod{12}$　　$x = 13, 25 \ldots$

PP106　由 $(x \bmod m_1, \ldots, x \bmod m_r)$ 确定 $(x \bmod m)$

$m \perp n$　求 a, b s.t

$a \bmod m = 1$　　$a \bmod n = 0$

$b \bmod m = 0$　　$b \bmod n = 1$

用 (4.5) Euclid 算法 求 m', n'

$$m'm + n'n = 1$$

$a = n'n$　　$b = m'm$

如有需要, 将二者对 mod mn 化简

12. Simplify the formula $\Sigma_{d\mid m} \Sigma_{k\mid d}\ \mu(k)\, g(d/k)$

13, **13** A positive integer n is called *squarefree* if it is not divisible by m^2 for any $m > 1$. Find a necessary and sufficient condition that n is squarefree,

a in terms of the prime-exponent representation (4.11) of n;

b in terms of $\mu(n)$.