1 令 $n=2^a3^b5^c$，它的因子个数为 $k=(a+1)(b+1)(c+1)$。所以 $k=1,2,3,4,5,6$ 时对应的 $n=1,2,4,6,16,12$

2 $Gcd(n,m)*Lcm(n,m)=n*m$. 因为对于某个素数 p，m,n 中 p 的个数的最小值最大值分别在最大公约数和最小公倍数中
$Gcd((n)mod(m),m)*Lcm((n)mod(m),m)=(n)mod(m)*m$
$Gcd(n,m)=Gcd((n)mod(m),m)$
$\Rightarrow Lcm(n,m)=Lcm((n)mod(m),m)*\frac{n}{(n)mod(m)}$

3 x 是整数时满足，x 为实数时 $\pi(x)-\pi(x-1)=[\lfloor x\rfloor\ is\ prime]$

4 depth1: $\frac{1}{1},\frac{1}{-1},\frac{-1}{-1},\frac{-1}{1}$
depth2: $\frac{1}{2},\frac{2}{1},\frac{2}{-1},\frac{-1}{-2},\frac{-2}{-1},\frac{-2}{1},\frac{-1}{2}$
如果把分子分母看作一个二维向量的话，每一层都是顺时针排列的。

5
$L^k=\begin{bmatrix}1 & k\\ 0 & 1\end{bmatrix}$
$R^k=\begin{bmatrix}1 & 0\\ k & 1\end{bmatrix}$

6 $(x)mod(0)=x\rightarrow a=b$

7 m 需要满足 $(m)mod(10)=0,(m)mod(9)=k,(m)mod(8)=1$
$(m)mod(10)=0$ 说明 m 是偶数，$(m)mod(8)=1$ 说明 m 是奇数。这是矛盾的。

8 $9x+y=3k,10x=5p$. 这说明 y 可以取 0,3，x 可以取 0,1.

9 $3^{2t+1}mod(4)=3$。所以 $3^{2t+1}=4k+3$. 所以 $\frac{3^{2t+1}-1}{2}=2k+1$ 是奇数。
另外 $\frac{3^{77}-1}{2}$ 可以被 $\frac{3^7-1}{2}$ 整除。因为 $3^{77}-1=(3^7-1)(3^{70}+3^{63}+..+3^7+3^0)$

10 $999=3^337^1\rightarrow\varphi(999)=999(1-\frac{1}{3})(1-\frac{1}{37})=648$

11 $f(n)=g(n)-g(n-1)\rightarrow\sigma(0)=1,\sigma(1)=-1,\sigma(n)=0,n>1$

12 $\sum_{d|m}\sum_{k|d}\mu(k)g(\frac{d}{k})=\sum_{d|m}\sum_{k|d}\mu(\frac{d}{k})g(k)=\sum_{k|m}\sum_{d|\frac{m}{k}}\mu(d)g(k)=\sum_{k|m}g(k)*[\frac{m}{k}=1]=g(m)$

13 n 的每个质因子个数都是 1.（1）$n_p\leq 1$ (2) $\mu(n)\neq 0$

14 $k>0$ 时两个都成立。

15 很明显 5 不是任何 e_n 的因子。首先对于模 5 来说，$e_1=2,e_n=e_{n-1}^2-e_n+1$, 所以这个模的结果依次是 2,3,2,3, 不会出现 0.

16 $\frac{1}{e_1}=\frac{1}{2},\frac{1}{e_1}+\frac{1}{e_2}=\frac{5}{6},\frac{1}{e_1}+\frac{1}{e_2}+\frac{1}{e_3}=\frac{41}{42}$，由此猜测 $\sum_{i=1}^k\frac{1}{e_i}=\frac{e_{k+1}-2}{e_{k+1}-1}$

假设前 n 项都成立，即 $\sum_{i=1}^n\frac{1}{e_i}=\frac{e_{n+1}-2}{e_{n+1}-1}$

那么 $\sum_{i=1}^{n+1}\frac{1}{e_i}=\frac{e_{n+1}-2}{e_{n+1}-1}+\frac{1}{e_{n+1}}=\frac{(e_{n+1}-1)e_{n+1}-1}{(e_{n+1}-1)e_{n+1}}=\frac{e_{n+2}-2}{e_{n+2}-1}$

17 $Gcd(f_m,f_n)=Gcd(f_m,(f_n)mod(f_m))=Gcd(f_m,2)=1$

18 如果 $n=rm$ 且 r 为奇数，那么有 $2^n+1=(2^m+1)(2^{n-m}-2^{n-2m}+2^{n-3m}-...+1)$，比如 $2^{12}+1=(2^4+1)(2^8-2^4+1)$

19 $\left\lfloor\frac{\varphi(k+1)}{k}\right\rfloor=1$ 当且仅当 $k+1$ 为素数。所以第一个式子表示 $[2,n]$ 中素数的个数，即 $\pi(n)$
第二个式子 $\sum_{1\leq k<m}\left\lfloor\frac{\frac{m}{k}}{\lceil\frac{m}{k}\rceil}\right\rfloor$ 当且仅当 m 为素数时等于 1, 否则大于 1。所以也表示 $\pi(n)$
$((k-1)!+1)mod(k)=0$ 当且仅当 k 为素数。所以也表示 $\pi(n)$

20 $p_1=2$。令 p_n 是满足大于 $2^{p_{n-1}}$ 的最小素数，那么有 $2^{p_{n-1}}<p_n<2^{1+p_{n-1}}$, 那么 $b=lim_{n\rightarrow oo}lg^{(n)}p_n$

21 由上面的题目 20 可以得到 $p_n < 10^n$. 证明如下

- 首先 $n=1$ 时满足，有 $2<10$
- 在 $(10^n, 2*10^n]$ 之间一定存在一个素数，所以 $p_{n+1} \le 2*10^n < 10^{n+1}$

因此 $K=\sum_{k\ge1}\frac{p_k}{10^{k^2}}=\frac{2}{10}+\frac{3}{10^4}+\frac{5}{10^9}+....$

22 假设含有 t 个 $1.(111..11)_b=\frac{b^t-1}{b-1}$。如果 t 不是素数，设 $t=nm$，那么 $\frac{b^t-1}{b-1}=\frac{b^{mn}-1}{b-1}=\frac{b^m-1}{b-1}*(b^{nm-m}+b^{nm-2m}+...+1)$

23 $\rho(2k+1)=0, \rho(2k)=\rho(k)+1$.
假设盘子的编号为 $0,1,2,...,n-1$，第 k 次移动的盘子编号为 $\rho(k)$, 可以用数学归纳法证明

24 假设 $n=\sum_{k=0}^{m-1}d_kp^k(0\le d_k<p)$
那么第 k 位对 $\varepsilon_p(n!)$ 的贡献为 $d_k(1+p+..+p^{k-1})=\frac{d_k(p^k-1)}{p-1}$, 累加所有项可以得到 $\varepsilon_p(n!)=\frac{n-\nu_p(n)}{p-1}$

25 (1)a 成立：有 $m\setminus\backslash n \leftrightarrow m_p=0||m_p=n_p$. 另外 m,k 互质，则对应的素数因子互不影响
(2) 在 $n=12, m=18$ 时 b 不成立

26 是的，因为 G_n 是 Stern-Brocot 的一个子树。因为如果一个 Stern-Brocot 的结点属于 G_n，那么这个结点的两个父节点也属于 G_n, 并且他们是小于和大于这个结点的结点中与这个节点最靠近的。

27 首先如果两个字符串一样长，那么只需要按照字符串比较大小即可。否则，可以在较短的一个串后面补字符 M 直到长度相等然后按照字符串大小比较即可。补 M 是因为一个结点左孩子都小于当前结点，右孩子都大于当前结点，而 M 正好满足 $L<M<R$

28 $\frac{1}{0},\frac{1}{1}$
$R^3:\frac{2}{1},\frac{3}{1},\frac{4}{1}$， 每次加上 $\frac{1}{0}$
$L^7:\frac{7}{2},\frac{10}{3},\frac{13}{4},\frac{16}{5},\frac{19}{6},\frac{22}{7},\frac{25}{8}$, 每次加上 $\frac{3}{1}$
就这样，下一行的分子分母的公差为上一行倒数第二个数字的分子分母, 因为那个是它的左祖先

29 对于 $[0,1)$ 中的数字 x 来说，$1-x$ 的二进制就是 x 的二进制表示中将 01 交换，因为 $1=\sum_{k>0}\frac{1}{2^k}$. 那么对于 $(0,\infty)\quad\alpha$ 来说，交换 LR 就是 $\frac{1}{\alpha}$。因为 Stern-Brocot 中对称的数字恰好是互为倒数。所以 $1-x$ 对应于 $\frac{1}{\alpha}$

30 $[A,A+m)$ 中的数字 x 模 m 各不相同，所以 r 元组 $((x)(mod)(m_1),(x)(mod)(m_2),..,(x)(mod)(m_r))$ 各不相同。所以总有一个元组是 $((a_1)(mod)(m_1),(a_2)(mod)(m_2),..,(a_r)(mod)(m_r))$

31 $(b)mod(d)=1\to(b^m)mod(d)=((kd+1)^m)mod(d)=1$
所以 $((a_ma_{m-1}...a_1a_0)_b=\sum_{k=0}^m a_kb^k)mod(d)=\sum_{k=0}^m a_k$ 也就是说，只要 $(b)mod(d)=1$，那么一个 b 进制的数字能够被 d 整除当且仅当各位数字之和能够被 d 整除

32 假设 $n\perp m$. 那么下面两个集合相等.
$\{(kn)mod(m)|k\perp m,1\le k<m\}=\{k|k\perp m,1\le k<m\}$
所以将两边的 $\varphi(m)$ 个数字乘起来，两边除以 $\prod_{k\perp m,0\le k<m}k$ 即可

33 $h(1)=1$, 假设 $n\perp m$, 那么 $h(mn)=\sum_{d\perp mn}f(d)g(\frac{mn}{d})=\sum_{x\perp m,y\perp n}f(xy)g(\frac{m}{x}\frac{n}{y})=\sum_{x\perp m}\sum_{y\perp n}f(x)g(\frac{m}{x})f(y)g(\frac{n}{y})=h(n)h(m)$

34 在公式 4.56 中，如果 d 不是整数，那么 $f(d)=0$, 所以 $g(m)=\sum_{d|m}f(d)=\sum_{d|m}f(\frac{m}{d})=\sum_{d\ge1}f(\frac{m}{d})$

35 下面使用的符号与公式 4.5 相关的符号相同。
$m^{'}=\overline{m}-\lfloor\frac{n}{m}\rfloor\overline{r}, n^{'}=\overline{r}\to I(m,n)=m^{'}=I(m,\overline{r})-\lfloor\frac{n}{m}\rfloor I(\overline{r},m)=I(m,(n)mod(m))-\lfloor\frac{n}{m}\rfloor I((n)mod(m),m), I(n,m)=n^{'}=(n)mod(m)$
$I(0,n)=0, I(m,0)=1$

36 首先证明 2 不可以。
假设 2 可以分解为两个非单位数乘积，即 $2=(a+b\sqrt{10})(c+d\sqrt{10})=(ac+10bd)+(ad+bc)\sqrt{10}\to ac+10bd=2, ad+bc=0\to(a-b\sqrt{10})(c-d\sqrt{10})=(ac+10bd)-(ad+bc)\sqrt{10}=2\to(a^2-10b^2)(c^2-10d^2)=4$

由于 $|a^2-10b^2|\neq 1,|c^2-10d^2|\neq 1$, 所以要么它们都为 2 或者都为-2.
由于任何整数的平方模 10 为 0,1,4,5,6,9, 所以不会是 2. 所以 $(a^2-10b^2)mod(10)=(a^2)mod(10)\neq 2$。所以假设错误。
3 和 $4\pm\sqrt{10}$ 的证明类似

37 令 $a_n=2^{-n}ln(e_n-\frac{1}{2})=2^{-n}ln((e_{n-1}-\frac{1}{2})^2+\frac{1}{4})>2^{-n}ln((e_{n-1}-\frac{1}{2})^2)=2^{-(n-1)}ln(e_{n-1}-\frac{1}{2})=a_{n-1}$
令 $b_n=2^{-n}ln(e_n+\frac{1}{2})=2^{-n}ln(e_{n-1}^2-e_{n-1}+\frac{3}{2})<2^{-n}ln(e_{n-1}^2+e_{n-1}+\frac{1}{4})=2^{-n}ln((e_{n-1}+\frac{1}{2})^2)=b_{n-1}$
所以 $a_{n-1}<a_n<b_n<b_{n-1}$
另外 $e_n=\lfloor E^{2^n}+\frac{1}{2}\rfloor\Leftrightarrow e_n\leq E^{2^n}+\frac{1}{2}<e_n+1\Leftrightarrow e_n-\frac{1}{2}\leq E^{2^n}<e_n+\frac{1}{2}\Leftrightarrow 2^{-n}ln(e_n-\frac{1}{2})\leq lnE<2^{-n}ln(e_n+\frac{1}{2})\Leftrightarrow a_n\leq lnE<b_n$
所以 $E=\lim_{n\to oo}e^{a_n}$

38 令 $r=(n)mod(m)$，那么 $a^n-b^n=(a^m-b^m)(a^{n-m}+a^{n-2m}b^m+...+a^rb^{n-m-r})+b^{m\lfloor\frac{n}{m}\rfloor}(a^r-b^r)$
所以 $Gcd(a^n-b^n,a^m-b^m)=Gcd((a^n-b^n)mod(a^m-b^m),a^m-b^m)=Gcd(b^{m\lfloor\frac{n}{m}\rfloor}(a^r-b^r),a^m-b^m)$
因为 $a\perp b\to b^m\perp(a^m-b^m)\to b^{m\lfloor\frac{n}{m}\rfloor}\perp(a^m-b^m)$
所以 $Gcd(b^{m\lfloor\frac{n}{m}\rfloor}(a^r-b^r),a^m-b^m)=Gcd(a^r-b^r,a^m-b^m)$
一直这样下去可以得到 $Gcd(a^n-b^n,a^m-b^m)=a^{Gcd(n,m)}-b^{Gcd(n,m)}$

39 假设相等，设 m 的序列为 $S_m=\{m,a_1,a_2,...,a_t,S(m)\}$,$m'$ 的序列为 $S_{m'}=\left\{m',b_1,b_2,...,b_u,S(m)\right\}$，令 $\{m,a_1,a_2,...,a_t,S(m)\}\cap\left\{m',b_1,b_2,...,b_u,S(m)\right\}=\{c_1,c_2,..,c_k,S_m\}=U$
所以 $\frac{\prod_{x\in S_m}x\prod_{y\in S_{m'}}y}{\prod_{x\in U}x^2}$ 也是完全平方数，所以这时候 $S(m)$ 不是最小的

40 这里的 p 是一个素数。
令 $f(n)=\prod_{1\leq k\leq n,(k)mod(p)\neq 0}k=\frac{n!}{p^{\lfloor\frac{n}{p}\rfloor}\lfloor\frac{n}{p}\rfloor!}$
那么 $\frac{n!}{p^{\xi_p(n!)}}=f(n)f(\left\lfloor\frac{n}{p}\right\rfloor)f(\left\lfloor\frac{n}{p^2}\right\rfloor)...$
而 $f(n)\equiv a_0!((p-1)!)^{\lfloor\frac{n}{p}\rfloor}\equiv a_0!(-1)^{\lfloor\frac{n}{p}\rfloor}(mod(p))$
$f(\left\lfloor\frac{n}{p}\right\rfloor)\equiv a_1!(-1)^{\left\lfloor\frac{n}{p^2}\right\rfloor}(mod(p))$
$f(\left\lfloor\frac{n}{p^2}\right\rfloor)\equiv a_2!(-1)^{\left\lfloor\frac{n}{p^3}\right\rfloor}(mod(p))$
乘起来可以得到 $\frac{n!}{p^{\xi_p(n!)}}\equiv(-1)^{\xi_p(n!)}a_0!a_1!..a_m!(mod(p))$

41 (1) 假设 $n^2\equiv -1(mod(p))\to(n^2)^{\frac{p-1}{2}}=n^{p-1}\equiv -1(mod(p))$, 这是矛盾的
（2） $n=(\frac{p-1}{2})!$
比如 $p=13$，那么 $(1)mod(13)=(-12)mod(13),(2)mod(13)=(-11)mod(13),..,(6)mod(13)=(-7)mod(13)$,
所以 $n\equiv\left((-1)^{\frac{p-1}{2}}\prod_{1\leq k\leq\frac{p-1}{2}}(p-k)=\frac{(p-1)!}{n}\right)(mod(p))\to n^2\equiv((p-1)!=1)\,(mod(p))$

42 A:$\frac{mn'+m'n}{nn'}$ 是最简分数
B: $n\perp n'$
A→ B: 假设 n,n' 不互质，设 $a=Gcd(n,n')>1$, 那么 $n=pa,n'=qa$, 所以 $mn'+m'n$ 和 nn' 一定有公约数 a. 假设失败。所以一定有 $n\perp n'$
B→ A: 假设 $a=Gcd(mn'+m'n,nn')>1$, 由于 $n\perp n'$, 不妨设 $n=pa,a\perp n',a\perp m$. 所以 $a\perp mn',a|m'n$, 所以 $Gcd(mn'+m'n,a)=1$, 假设失败。所以 A 成立

43 函数 $\rho(n)$ 的递推公式在题目 23 中。
(1)n 为奇数时，$\begin{bmatrix}0&-1\\1&1\end{bmatrix}$=$L^{-1}R$。
(2)n 为偶数时，可以用数学归纳法证明 $\begin{bmatrix}0&-1\\1&2\rho(n)+1\end{bmatrix}$=$R^{-\rho(n)}L^{-1}RL^{\rho(n)}$. 不停用 $\rho(2k)=\rho(k)+1$ 展开，前面的式子等价于证明 $\begin{bmatrix}0&-1\\1&2k+1\end{bmatrix}=R^{-k}L^{-1}RL^k$. 前面一项以及乘以这个矩阵后的样子是分别是 $...L\underbrace{RR...R}_{\rho(n)}\to ...R\underbrace{LL...L}_{\rho(n)}$

44 数字 0.3155 和 0.3165 的分数是 $\frac{631}{2000},\frac{633}{2000}$。在 Stern-Brocot 中在这个区间中最简单的分数是 $\frac{6}{19}$

45 $x^2\equiv x(mod(10^n))\Leftrightarrow x(x-1)\equiv 0(mod(10^n))\Leftrightarrow x(x-1)\equiv 0(mod(2^n)),x(x-1)\equiv 0(mod(5^n))\Leftrightarrow(x)mod(2^n)=0,1,(x)mod(5^n)=0,1$
所以满足条件的 x 最多有四个，其中两个是 $0,1$，另外两个的形式为 $t,10^n+1-t$

46　(1) 假设 $j'j-k'k=Gcd(j,k)$，那么有 $n^{j'j}=n^{k'k}n^{Gcd(j,k)}$，所以如果 $n^{j'j}=pm+1, n^{k'k}=qm+1 \to n^{Gcd(j,k)}=rm+1$
(2) 假设 $n=pq$ 并且 p 是 n 的最小素因子（如果 n 为素数那么 $p=n$）。所以 $2^{p-1}\equiv 1(mod(p))$。
如果 $2^n\equiv 1(mod(n)) \to 2^n\equiv 1(mod(p))$。(如果 $2^n\not\equiv 1(mod(p))$, 不妨设为 x, 那么 $2^n=kp+x$. 如果仍然有 $2^n\equiv 1(mod(n)$, 那么有 $2^n=rn+1$, 所以 $(kp+x)-(rn+1)=(k-rq)p+(x-1)=0$, 显然不成立)
所以根据上面一个小题的结论,$2^{Gcd(p-1,n)}\equiv 1(mod(p))$。而由于 p 是 n 的最小素因子，所以 $Gcd(p-1,n)=1$。这会导致错误。所以 $2^n\not\equiv 1(mod(n))$

47 $n^{m-1}\equiv 1(mod(m)) \to n\perp m \to n^t\perp m \to ((n^t)mod(m))\perp m, 1\le t<m$
假设：如果对于所有的 $1\le t<m$，$(n^t)\,mod(m)$ 不是各不相同的，比如对 $1\le x<y<m$ 有 $((n^x)mod(m))=((n^y)mod(m))$，那么 $n^{y-x}\equiv 1(mod(m))$, 其中 $y-x<m-1$
根据题目 46 第一小题的结论，$n^{y-x}\equiv 1, n^{m-1}\equiv 1 \to n^{Gcd(y-x,m-1)}\equiv 1$，而 $Gcd(y-x,m-1)<m-1$.
令 $k=min(y-x,Gcd(y-x,m-1))$，那么 k 一定能整除 $m-1$. 所以存在一个素数 p 以及一个整数 q 满足 $kq=\frac{m-1}{p}$, 而 $\left(n^{\frac{m-1}{p}}=n^{kq}\right)\equiv 1$，而这与题目给出的 $n^{\frac{m-1}{p}}\not\equiv 1$ 矛盾了。所以上面的假设错误。
对于所有的 $1\le t<m$，$(n^t)\,mod(m)$ 各不相同，并且都与 m 互质，所以 $1,2,3,...,m-1$ 都与 m 互质，所以 m 是素数

48 将每个数字与其逆元相乘，得到 1. 所以可以不管这些数字。那么只剩下那些逆元是自己的数字，所以就是计算 $\prod_{1\le n<m,(n^2)mod(m)=1} n$. 根据 $n^2\equiv 1(mod(m))$ 的解可以得到，当 $m=4,p^k,2p^k(p>\ ,k\ge 1)$ 答案为- 1 ，否则为 1

49 (1) 首先考虑 $m<n$，此时答案为 $\Phi(N)=\left(\sum_{k=1}^{N}\varphi(k)\right)-1$,$m>n$ 也是这个，$m=n$ 时只有 $m=n=1$ 成立，所以答案为 $R(N)=2\Phi(N)-1$
(2) 由公式 4.62 可以得到 $R(N)=2\Phi(N)-1=-1+\sum_{d\ge 1}\mu(d)\left\lfloor\frac{N}{d}\right\rfloor\left\lfloor\frac{N}{d}+1\right\rfloor=\sum_{d\ge 1}\mu(d)\left\lfloor\frac{N}{d}\right\rfloor^2+\left(\sum_{d\ge 1}\mu(d)\left\lfloor\frac{N}{d}\right\rfloor-1\right)$
所以现在只需要满足 $\sum_{d\ge 1}\mu(d)\left\lfloor\frac{N}{d}\right\rfloor=1$ 即可
在公式 4.61 中，令 $f(x)=[x\ge 1] \to g(N)=\sum_{d\ge 1}[\frac{N}{d}\ge 1]=N \to \sum_{d\ge 1}\mu(d)\left\lfloor\frac{N}{d}\right\rfloor=\sum_{d\ge 1}\mu(d)g(\left\lfloor\frac{N}{d}\right\rfloor)=\sum_{d\ge 1}\mu(d)g(\frac{N}{d})=f(N)=1$

50 (1) 设 f 是任意一个函数。$\prod_{0\le k<m}f(k)=\prod_{d|m}\prod_{0\le k<m}f(k)[d=Gcd(k,m)]=\prod_{d|m}\prod_{0\le k<m}f(k)[\frac{k}{d}\perp\frac{m}{d}]=\prod_{d|m}\prod_{0\le k<\frac{m}{d}}f(kd)[k\perp\frac{m}{d}]=\prod_{d|m}\prod_{0\le k<d}f(k\frac{m}{d})[k\perp d]$
所以 $z^m-1=\prod_{0\le k<m}(z-\omega^k)=\prod_{d|m}\prod_{0\le k<d,k\perp d}(z-\omega^{\frac{km}{d}})=\prod_{d|m}\Psi_m(z)$
最后一步成立是因为 $\omega^{\frac{km}{d}}=e^{\frac{2\pi i}{m}*\frac{km}{d}}=e^{\frac{2\pi i}{d}*k}$
(2) 如果令 $g(m)=z^m-1, f(m)=\Psi_m(z)$，也就是已知 $g_m=\prod_{d|m}f(d)$ 而证明 $f_m=\prod_{d|m}g(d)^{\mu(\frac{m}{d})}$，两边都取对数，就变成了公式 4.56