0.1 (a) $f = \Theta(g)$ (b) $f(n) = O(g(n))$

(c) 显然 $f(n) \le 100g(n)$ 但 $f(n) \ge 50g(n)$ $f(n) = \Theta(g(n))$

$cg(n) \le f(n) \le cg(n)$ (d) $f(n) = n\log n$ $g(n) = 10n\log n + 10\cdot\log 10\cdot n$.

$f(n) = \Theta(g(n))$

(e) $f(n) = \Theta(g(n))$ (f) $f(n) = \Theta(g(n))$ (g) $f(n) = \Omega(g(n))$

(h) $f(n) = \Omega(g(n))$ (i) $f(n) = \Omega(g(n))$ (j) $f(n) = n^{\log(\log n)}$. $f(n) = \Omega(g(n))$

(k) $f(n) = \Omega(g(n))$ (l) $n^{\frac{1}{2}}$ $g(n) = n^{\log_2 5}$. $f(n) = O(g(n))$

(m) $f(n) = O(g(n))$ (n) $f(n) = \Theta(g(n))$ (o) $f(n) = \Omega(g(n))$

(p) $f(n) = n^{\log(\log n)}$ $g(n) = n^{\log_2 n}$ $f(n) = O(g(n))$

(q) $$\frac{\sum_{i=1}^{n} i^k}{n^{k+1}} = \frac{1}{n}\sum_{i=1}^{n}\left(\frac{i}{n}\right)^k = \int_0^1 x^k\,dx = \frac{1}{k+1}.$$ $f(n) = \Theta(g(n))$

0.2. (a) $g(n) = \frac{1-c^n}{1-c}$. if $c < 1$:

$c^n \to 0$ $g(n) \to \frac{1}{1-c}$

故 $g(n) = \Theta(1)$

(b) $g(n) = n$. 显然

(c) $g(n) = \frac{c^n - 1}{c-1} \approx c^n \cdot \frac{1}{c-1}$.

1.14. $F_1 = F_1$ $F_2 = F_1 + F_0$ $\begin{pmatrix} F_1 \\ F_2 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} F_0 \\ F_1 \end{pmatrix}$

$\begin{pmatrix} F_2 \\ F_3 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^2 \cdot \begin{pmatrix} F_0 \\ F_1 \end{pmatrix}$ 故 $\begin{pmatrix} F_n \\ F_{n+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^n \cdot \begin{pmatrix} F_0 \\ F_1 \end{pmatrix}$

假设 n位数乘矩阵时间为 $x(n)$

在 0.4中 fib3调用 $O(\log n)$ 次乘法。 对于每次 mod P. 复杂度为 $O(\log P)$, 因为 $\log P$ bits.

所以, 最终复杂度为

$O(\log(n) \times x(\log P))$

$O(\log N \times n(\log P))$

1.31 (a) N 有 n bits 那么 $N!$ 有 $\Theta(n^2)$ 位.

$N! = 1 \cdot 2 \cdots N$. $\log_2(N!) = \Theta(N \log_2 N)$

所以可以写成 $N! = \Theta(N \log_2 N)$ 又显然 N 有 n bits

故 $N! = \Theta(2^n \cdot n)$

(b) 计算 $N!$:

```
Factorial(N)
    if N=1:
        ret 1
    else:
        ret N·Factorial(N-1)
```

建议 vector<int> dp(n)

不然会爆栈.

空间复杂度: $O(N \cdot \log N)$ $\log N$ 位. 每次复杂度 N.

1.35 N is prime $\Leftrightarrow (N-1)! \equiv -1 \pmod N$

(a) $\forall\, 0 \le x < p$ 都对 p.

$t^2 \equiv 1 \pmod p$ 故 $t^2 + (p-1)! \mid p$.

又有 $(p-1)! \equiv -1 \pmod p$ 显然 $t = p-1$ 和 $t = 1$ 满足.

p is prime

(b) 对于 prime p $(p-1)! \equiv -1 \pmod p$

如果是质数 $\gcd(a,n) > 1$ then $ax \not\equiv 1 \bmod n$.

if $p=2$. then $(p-1)! = 1 \equiv -1 \pmod 2$

for $p \ge 3$, 显然 $1 \cdot (p-1) \equiv -1 \pmod p$ $1, p-1$ 是关于自己的逆元.

那剩下 $p-1-2 = p-3$ 个数 以有 $\frac{p-3}{2}$ 个逆元对.

即 $\forall\, 2 \le x < p-1$, 必有 $2 \le y < p-1$ 且 $x \ne y$, 使 $xy \equiv 1 \pmod p$

故 $\prod_{i=1}^{p-1} i$, 即 $(p-1)! \equiv -1 \pmod p$

(c) $d = \gcd(N, (N-1)!)$ $(N-1)! \equiv \quad \pmod N$

let $N = ab$. $1 < a, b < N$.

显然 a, b 都在 $1 \sim N-1$ 中. then $(N-1)! \equiv 0 \pmod N \not\equiv -1 \pmod N$