31.1-10

设：$a=\prod_{i=1}^{n} p^{\alpha_i}$ $b=\prod_{i=1}^{n} p^{\beta_i}$ $c=\prod_{i=1}^{n} p^{\gamma_i}$

则：$gcd(a,gcd(b,c))=gcd\left(a,\prod_{i=1}^{n} p^{\max\{\beta_i,\gamma_i\}}\right)=gcd\left(\prod_{i=1}^{n} p^{\alpha_i},\prod_{i=1}^{n} p^{\max\{\beta_i,\gamma_i\}}\right)=\prod_{i=1}^{n} p^{\max\{\alpha_i,\beta_i,\gamma_i\}}$

同理：$gcd(gcd(a,b),c)=\prod_{i=1}^{n} p^{\max\{\alpha_i,\beta_i,\gamma_i\}}$

故：$gcd(a,gcd(b,c))=gcd(gcd(a,b),c)$

31.2-5

$$F_n=\frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n-\left(\frac{1-\sqrt{5}}{2}\right)^n\right]$$

$$b<F_{n+1}=\frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{n+1}-\left(\frac{1-\sqrt{5}}{2}\right)^{n+1}\right]<\left(\frac{1+\sqrt{5}}{2}\right)^n$$

即满足上面式子的最小 n 为：$\log_\phi b+1$

所以由 Lame 定理可知：EUCLID(a,b)至多执行$\log_\phi b+1$次递归调用。因为该算法达到 gcd(a,b)时终止，所以可以修改 Lame 定理的$b<F_{k+1}$为$b<gcd(a,b)\times F_{k+1}$，定理一样成立。同上证明，只是 b 变成了 b/gcd(a,b)。所以该函数至多运行了$\log_\phi\left(\frac{b}{gcd(a,b)}\right)+1$次递归调用。

31.4-1

$$35x\equiv 10\ (mod\ 50)\ \rightleftharpoons\ 7x\equiv 2\ (mod\ 10)$$

由： $7^{-1}\equiv 3\ (mod\ 10)$

$$x\equiv 2\times 7^{-1}\equiv 2\times 3\equiv 6\ (mod\ 10)$$

即： $x\equiv 6\ (mod\ 10)$ 为解

31.5-2
题意等价于:

$$x \equiv 1 \ (mod\ 9)$$
$$x \equiv 2 \ (mod\ 8)$$
$$x \equiv 3 \ (mod\ 7)$$

$$x = 9 \times 8 \times 3 \times M_3 + 9 \times 7 \times 2 \times M_2 + 7 \times 8 \times 1 \times M_1$$

$$M_1 \equiv (9 \times 8)^{-1} \equiv 4 \ (mod\ 7)$$
$$M_2 = (9 \times 7)^{-1} = 7 \ (mod\ 8)、$$
$$M_3 = (8 \times 7)^{-1} = 5 \ (mod\ 9)$$

$$x = 9 \times 8 \times 3 \times 4 + 9 \times 7 \times 2 \times 7 + 7 \times 8 \times 1 \times 5 \ (mod\ 7 \times 8 \times 9)$$

$$x \equiv 10 \ (mod\ 504)$$

31.7-2

$$ed \equiv 3d \equiv 1 \ (mod\ \phi(n))$$

$$3d = k \times \phi(n) + 1$$

由于 d 的范围限制，所以 k=1 或 k=2。

这样就可以解出来：$\phi(n) = \dfrac{3d-1}{k} = (p-1)(q-1)$　k=1 或 2

然而又知道：$n = pq$

以上两个式子联立 p、q 分别为:

$p,q = \left(n+1-\phi(n) \pm \sqrt{(n+1-\phi(n))^2 - 4n}\right)/2$

由于只涉及到了加减乘除开方平方运算，所以计算可以控制在 n 的位数的多项式时间。

31.8-3
由题意:

$$(x-1)(x+1) \equiv 0 \ (mod\ n)$$

非平凡表明 x mod n 不是 1 和 n-1。假设命题不成立，则两个数中至少存在一个平凡约数（1 或者 n），则可以知道 x-1 与 x+1 中至少有一个被 n 整除。
如果是 x-1，则 n|(x-1)，导出 x mod n 为 1，矛盾!
如果是 x+1，则 n|(x+1)，导出 x mod n 为 n-1，也矛盾!
所以假设不成立。即 gcd(x-1,n)与 gcd(x+1,n)都是 n 的非平凡约数。