hw11

> 31.1-10；31.2-5；31.4-1；31.5-2；31.7-2；31.8-3；

31.1-10

31.1-10 证明：最大公约数运算满足结合律，即证明对所有整数 a、b 和 c，

$$\gcd(a,\gcd(b,c))=\gcd(\gcd(a,b),c)$$

考虑a、b和c的质因数分解，写作a = p1p2...pk，其中允许质数重复。b和c的最大公约数（gcd）仅是同时出现在两个分解中的所有pi的乘积。如果它出现多次，我们将其包含在出现次数较少的一方的pi次数中。为了得到gcd(b, c)和a的最大公约数，我们再次进行这个过程。因此，左边是a、b和c的质因数乘积的交集（考虑到适当的重复性）。对于右边，我们首先考虑a和b的质因数的交集，然后是c的质因数，但由于交集是关联的，gcd运算也是关联的。

31.2-5

31.2-5 如果 $a>b\geqslant 0$，证明：EUCLID(a，b)至多执行 $1+\log_\phi b$ 次递归调用。把这个界改进为$1+\log_\phi(b/\gcd(a,b))$。

对于所有的k，如果 $b<F_{k+1}<\phi^{k+1}/\sqrt{5}$，那么需要的步骤少于 k 步。如果我们令 $k=\log_\phi b+1$，那么由于 $b<\phi^{\log_\phi b+2}/\sqrt{5}=\frac{\phi^2}{\sqrt{5}}\cdot b$，我们有它只需要 $1+\log_\phi(b)$ 步。

我们可以将这个界限改进为 $1+\log_\phi(b/\gcd(a,b))$。这是因为我们知道算法将在达到 $\gcd(a,b)$ 时终止。我们将模仿引理31.10的证明，来展示一个略有不同的命题，即欧几里得算法需要 k 次递归调用，则 $a\geq\gcd(a,b)F_{k+2}$ 和 $b\geq\gcd(a,b)F_{k+1}$。我们将对 k 进行归纳法证明。如果需要一次递归调用，并且我们有 $a>b$，那么 $a\geq 2\gcd(a,b)$ 且 $b=\gcd(a,b)$。

现在，假设它对 $k-1$ 成立，我们想证明它对 k 也成立。第一次调用的是 $\mathrm{EUCLID}(b,a \bmod b)$。由于此时只需要 $k-1$ 次递归调用，我们可以应用归纳假设得出 $b\geq\gcd(a,b)F_{k+1}$ 和 $a \bmod b\geq\gcd(a,b)F_k$。由于我们有 $a>b$，那么 $a\geq b+(a \bmod b)\geq\gcd(a,b)(F_{k+1}+F_k)=\gcd(a,b)F_{k+2}$，完成了归纳。

由于我们有只需要 k 步，只要 $b<\gcd(a,b)F_{k+1}<\gcd(a,b)\phi^{k+1}$，我们得出 $\log_\phi(b/\gcd(a,b))<k+1$。如果我们设定 $k=1+\log_\phi(b/\gcd(a,b))$，这个条件就得到满足。

31.4-1

31.4-1 找出方程 $35x\equiv 10 \pmod{50}$ 的所有解。

根据题述，首先对35和50运行扩展欧几里得算法，得到的结果是 $(5,-7,10)$。这里的结果表示35和50的最大公约数是5，且存在整数对$(-7,10)$使得 $35(-7)+50(10)=5$。

然后，根据这些信息来找到初始解。初始解是 $-7\times\frac{10}{5}=-14$。但是，由于我们通常希望解为正数或零，可以将这个解调整到最接近的50的倍数范围内。-14 加上50的倍数可以得到正解，

因此第一个正解是 $-14+50=36$。

由于$d=5$，解集中有其他四个解，对应于加上 $50/5=10$ 的倍数。因此，整个解集是 $x=\{36,36-10,36-20,36-30,36-40\}$，即 $x=\{36,26,16,6,-4\}$。但是，如果我们只考虑非负解，则解集应为 $x=\{6,16,26,36\}$。

因此，最终的非负解集是 $x=\{6,16,26,36\}$。

31.5-2

31.5-2 找出被 9，8，7 除时，余数分别为 1，2，3 的所有整数 x。

由于$9\cdot 8\cdot 7=504$，我们就以 $mod504$ 来进行分析。另外有$m1=56,m2=63,m3=72.$ 计算得$c1=56(5)=280,c2=63(7)=441,c3=72(4)=288.$ 所以 $a=280+2(441)+3(288)\ mod504=10\ mod\ 504$。由此得我们希望有的整数是 $x=10+504k,k\in Z.$

31.7-2

31.7-2 证明：如果 Alice 的公开指数 e 等于 3，并且对方获得了 Alice 的秘密指数 d，其中 $0<d<\phi(n)$，则对方能够在关于 n 的位数的多项式时间内对 Alice 的模 n 进行分解。(尽管不用证明下列结论，但你也许会对下列事实感兴趣：即使条件 $e=3$ 被去除，上述结论仍然成立。参见 Miller[255]。)

在给定 $ed\equiv 1 \pmod{\phi(n)}$ 的情况下，由于 $d<\phi(n)$ 且 $e=3$，我们得出 $3d-1=k(p-1)(q-1)$，其中 $k=1$ 或 $k=2$。这里的 p 和 q 是大素数，$n=pq$ 是它们的乘积，而 $\phi(n)=(p-1)(q-1)$ 是欧拉函数 ϕ 在 n 上的值。

对于 k 的确定，如果 $3d-1<n$，则 $k=1$；如果 $3d-1>n$，则 $k=2$。一旦确定了 k，就可以根据公式 $p+q=n-\frac{3d-1}{k}+1$ 来求解 $p+q$。这个过程的时间复杂度是多项式级别的，因为在求解时仅涉及加法、乘法和除法，且操作数不超过 n。

接下来，通过替换我们之前的方程中的 $q-1$ 为 $(p+q)-p-1$，可以在多项式时间内求解 p。这一步同样涉及基本算术运算，并且操作数同样受到 n 的限制。

综上，这种方法允许在多项式时间内求解出 p 和 q，这在某些密码学应用中，如RSA加密算法的密钥破解，是非常关键的。然而，值得注意的是，实际上找出 p 和 q 通常需要更复杂的方法，特别是当 n 非常大时。

31.8-3

31.8-3 证明：如果 x 是以 n 为模的 1 的非平凡平方根，则 $\gcd(x-1, n)$和 $\gcd(x+1, n)$都是 n 的非平凡约数。

首先，证明以下引理。对于任意整数 $a,b,n,\gcd(a,n)$ 和 $\gcd(b,n)\geq\gcd(ab,n)$。设 $\{p_i\}$ 是素数的枚举，那么根据定理31.8，存在唯一一组素数的幂次，使得 $a=\prod_i p_i^{a_i},b=\prod_i p_i^{b_i}$，以及 $n=\prod_i p_i^{n_i}$。

$$\gcd(a,n) = \prod_i p_i^{\min(a_i,n_i)}$$
$$\gcd(b,n) = \prod_i p_i^{\min(b_i,n_i)}$$
$$\gcd(ab,n) = \prod_i p_i^{\min(a_i+b_i,n_i)}$$

将前两个等式结合起来，得到：

$$\begin{aligned}\gcd(a,n)\cdot\gcd(b,n) &= \left(\prod_i p_i^{\min(a_i,n_i)}\right)\cdot\left(\prod_i p_i^{\min(b_i,n_i)}\right)\\ &= \prod_i p_i^{\min(a_i,n_i)+\min(b_i,n_i)}\\ &\geq \prod_i p_i^{\min(a_i+b_i,n_i)}\\ &= \gcd(ab,n)\end{aligned}$$

由于 x 是非平凡的平方根，我们有 $x^2 \equiv 1 \pmod{n}$，但 $x \neq 1$ 且 $x \neq n-1$。现在，考虑 $\gcd(x^2-1,n)$ 的值。根据定理31.9，这等于 $\gcd(n, x^2-1 \bmod n) = \gcd(n, 1-1) = \gcd(n,0) = n$。因此，可以观察 $x^2-1=(x+1)(x-1)$ 的因式分解，得到：

$$\gcd(x+1,n)\cdot\gcd(x-1,n) \geq n$$

然而，我们知道由于 x 是非平凡的平方根，$1 < x < n-1$，所以等式右边的两个因子都不可能等于 n。这意味着右边的两个因子都必须是非平凡的。