应用密码学第二次作业解答

1. 试编写一段程序实现扩展欧几里得算法。

解： 算法伪代码：

```
# 给定正整数a，b，计算gcd(a,b)和Bézout系数s，t，使得gcd(a,b)=sa+tb
function extended_gcd(a, b)
  s := 0;    old_s := 1;
  t := 1;    old_t := 0;
  r := b;    old_r := a;

  while r != 0
    quotient := old_r div r
    (old_r, r) := (r, old_r - quotient * r)
    (old_s, s) := (s, old_s - quotient * s)
    (old_t, t) := (t, old_t - quotient * t)

  output "Bézout coefficients:", (old_s, old_t)
  output "greatest common divisor:", old_r
```

2. 试证同余方程

$$a_1x_1 + \cdots + a_nx_n \equiv b \pmod m$$

有解$(x_1, \ldots, x_n)$ 之充分必要条件为$(a_1, \ldots, a_n, m) \mid b$. 若此条件适合, 则其解的个数(对模$m$ 不同余者) 为

$$m^{n-1}(a_1, \ldots, a_n, m).$$

证明： (必要性) 若方程$a_1x_1 + \cdots + a_nx_n \equiv b \pmod m$有解，则存在整数$(s_1, \ldots, s_n, k)$满足

$$a_1s_1 + \cdots + a_ns_n + km = b.$$

由于$(a_1,\dots,a_n,m)\mid a_i$，$(a_1,\dots,a_n,m)\mid m$，从而$(a_1,\dots,a_n,m)\mid b$.

(充分性) 利用归纳法和扩展欧几里得算法容易得到存在整数$(s_1,\dots,s_n,k)$ (Bèzout系数) 使得

$$(a_1,\dots,a_n,m)=a_1s_1+\cdots+a_ns_n+km.$$

由$(a_1,\dots,a_n,m)\mid b$可知方程$a_1x_1+\cdots+a_nx_n\equiv b \pmod m$存在一组解

$$\left(\frac{b}{(a_1,\dots,a_n,m)}s_1,\dots,\frac{b}{(a_1,\dots,a_n,m)}s_n\right).$$

再计算解的个数。首先，容易发现，若方程$a_1x_1+\cdots+a_nx_n\equiv b \pmod m$有解，则其 $\mathrm{mod}\ m$不同余的解的个数等于方程$a_1x_1+\cdots+a_nx_n\equiv 0 \pmod m$的解的个数；其次，设$d=(a_1,\dots,a_n,m)$，容易证明方程$\frac{a_1}{d}x_1+\cdots+\frac{a_n}{d}x_n\equiv 0 \pmod{\frac{m}{d}}$的$\mathrm{mod}\ \frac{m}{d}$不同余的解分别对应着方程$a_1x_1+\cdots+a_nx_n\equiv 0 \pmod m$的$d^n$个$\mathrm{mod}\ m$不同余的解(请自行验证)。

注意到$\left(\frac{a_1}{d},\dots,\frac{a_n}{d},\frac{m}{d}\right)=1$，因此可将问题归结为研究方程$a_1x_1+\cdots+a_nx_n\equiv 0 (\mathrm{mod} m)$在满足$(a_1,\dots,a_n,m)=1$时的解的个数。若$m=p^u$，$p$为素数，则存在$j$使得$(a_j,m)=1$，从而有$a_jx_j\equiv -\sum_{i\neq j}a_ix_i \pmod m$。注意到对任意$x_i\ (i\neq j)$的取值，该方程有唯一解（$\mathrm{mod}\ m$的意义下），从而方程解的总数为$m^{n-1}$。根据中国剩余定理可知对一般的$m$，所要考查方程的解数为$m^{n-1}$。最终可得原方程解的个数为

$$d^n\left(\frac{m}{d}\right)^{n-1}=dm^{n-1}.$$

□

方程解的个数也可以使用数学归纳法证明。从代数的角度，考查方程$a_1x_1+\cdots+a_nx_n\equiv b(\mathrm{mod} m)$解的情况，相当于考查在环$\mathbb{Z}/(m)$中理想$(a_1,\dots,a_n)$是否包含$b$。由于$\mathbb{Z}/(m)$为主理想环，容易证明$(a_1,\dots,a_n)=(d)$，其中$d=(a_1,\dots,a_n,m)$，故当$d\mid b$时$b\in(d)$，同余方程有解。为了计算解的个数，考查满同态

$$\psi:\ (\mathbb{Z}/(m))^n\longrightarrow(d)\qquad (x_1,\dots,x_n)\longmapsto\sum_{i=1}^n a_ix_i.$$

根据同态基本定理可得

$$|\ker\psi| = |(\mathbb{Z}/(\mathrm{m}))^{\mathrm{n}}|/|(\mathrm{d})| = \frac{\mathrm{m}^{\mathrm{n}}}{\mathrm{m}/\mathrm{d}} = \mathrm{dm}^{\mathrm{n}-1}.$$

3. 二数余一，五数余二，七数余三，九数余四，问本数。

解： 根据中国剩余定理可求得$x \equiv 157 \pmod{630}$.