关于px+qy类命题的研究

华南师大附中 袁豪

命题1：已知$(p,q)=1$，$p\ge1,q\ge1$，求证不能表示为$px+qy,(x\ge0,y\ge0)$的最大整数是$pq-p-q$。（如无特别说明，这里所有字母都是整数）

证：

首先证明：$pq-p-q$不能表示为$px+qy$的形式

反证法：假设存在$x\ge0$，$y\ge0$使$pq-p-q = px + qy$，则有

$pq-p-q = px + qy$

$p(q-x-1)=q(y+1)$

$q \mid q-x-1$ （因为 $(p,q)=1$）

$q \mid x+1$

又因为 $px=pq-p-q-qy <pq$ 所以 $x<q$ $x\le q-1$

由 $0\le x\le q-1$ 以及 $q \mid x+1$ 可以得到：$x=q-1$，

有 $pq-p-1=px+qy=p(q-1)+qy$ $y=-1$，这与 $y\ge0$ 矛盾

故$pq-p-q$不能表示为 $px+qy$，$(x\ge0,y\ge0)$

现在证明：对于 $n>pq-p-q$，必定存在$x\ge0$，$y\ge0$使$n=px+qy$

考察这样q个数：

n

$n-p$

$n-2p$

$n-3p$

…

$n-(q-1)p$

这个q个数除以q的余数必定构成集合$\{0,1,2,\ldots,q-1\}$，

否则必存在$0\le i<j\le q-1$使 $q \mid (n-ip)-(n-jp)$ $q \mid (j-i)p$ $q\mid j-i$

但是 $1\le j-i\le q-1$，所以不可能有$q\mid j-i$，

于是这个q个数除以q的余数必定构成集合$\{0,1,2,\ldots,q-1\}$，

如果 $n-up$ （v为整数）除以q的余数为0，设 $n-up=vq$，$(0\le u\le q-1)$，

由于 $vq=n-up>(pq-p-q)-(q-1)p = -q$ $v>-1$ $v>=0$，

所以y取v，x取u即得$px+qy=n$

证毕。

推论1：已知 $(A1,A2,A3,\ldots,As) = 1$，$Ai\ge1$ $(1\le i\le s)$，Ai互不相等，则对于$n>\prod Ai-\sum Ai$，必定存在$Xi\ge0$ $(1\le i\le s)$，使 $n=\sum AiXi$

证：可用数学归纳法证明，请同学们自己尝试。（这个推论比较弱）

命题2：已知 $(p, q) = 1$，$p\ge1,q\ge1$，对于任意非负整数n都能表示为$pu + qv$，$(0\le u\le q-1)$。

证1：由命题1的证明即可

证2：由于存在整数x,y使 $n=px+qy$，所以由恒等式：

$n=px+qy=p(x+qt)+q(x-pt)=p(x-qt)+q(x+pt)$ 可以调整出符合命题的u、v

来

推论 2：已知 (p , q) = 1 , p≥1,q≥1，记 m=pq-p-q，对于 n (0≤n≤m)和 m-n，其中有且只有一个能表示为 px+qy (x≥0,y≥0)的形式。
证：由命题 2 知 n,m-n 可以分别表示为：
  n=px+qy (0≤x≤q-1)
m-n=pu+qv (0≤u≤q-1)
相加得
   m=p(x+u)+q(y+v)
   pq-p-q=px+u)+q(y+v)
   p(q-1-x-u)=q(y+v+1)
   q|(q-1-x-u) 且 p|(y+v+1)
q|(q-1-x-u)   q|x+u+1
因为 1≤x+u+1≤2q-1 所以 x+u+1=q
故 y+v+1=0 在这里我们得到了 x 和 u 与 y 和 v 的关系式
如果 y、v 都小于 0，那么 0=1+y+v<=1+(-1)+(-1)=-1，这是不可能的
如果 y、v 都不小于 0，那么 0=1+u+v>=1，这也是不可能的
所以 y、v 中有一个小于 0，有一个不小于 0
也就是说 n 和 m-n 中有一个能表示为 px+qy (x≥0,y≥0)的形式，另一个则不能。
证毕。

推论 3：已知 (p,q)=1 , p≥1,q≥1，则不能表示为 px+qy (x≥0,y≥0)的形式的非负整数的数目为 (p-1)(q-1)/2
证：首先 p,q 不同时为偶数，所以 pq-p-q+1=(p-1)(p-1)必为偶数
由推论 2 知：在[0,pq-p-q]内的 pq-p-q+1 个整数，按和为 pq-p-q 配对，共得(pq-p-q+1)/2 对，每一对必有一个不能表示为题目所述形式。而对于大于 pq-p-q 的整数，由命题 1 知必定能表示为那种形式。所以不能表示为那种形式的非负整数的数目为 (p-1)(q-1)/2

问题：已知 p,q，求 n=(p,q)，以及 满足 px+qy=n 的 x,y
算法：辗转相处法。
y=(n-px)/q=(n-(p mod q)x)/q-(p div q)x
记 y'=x, x'=(n-(p mod q)x)/q=(n-(p mod q)y')/q
   qx'+(p mod q)y'=n
于是我们可以递归的得到 x' 和 y'
然后得出
x=y'
y=x'-(p div q)y'
附 Pascal 程序：
```
function extended_euclid(p,q:longint; var x,y:longint):longint;
var
  t:longint;
begin
  if q=0 then
```

```
  begin
    extended_euclid:=p;
    x:=1;
    y:=0;
  end else
  begin
    extended_euclid:=extended_euclid(q,p mod q,x,y);
    t:=x;
    x:=y;
    y:=t-p div q*y;
  end;
end;
```

总结：这些结论对解一些数论问题有很大的帮助。