问题求解（三）第13周作业

黄奕诚161220049

November 27, 2017

TC Chapter 31

31.1-12

Algorithm 1 BIT-DIVISION(a,b)

$BitNum_a$ and $BitNum_b$ is the bit numbers of a and b
$quotient \leftarrow 0$
for $i \leftarrow BitNum_a - BitNum_b$ **to** 0 **do**
  $m \leftarrow (b << i)$
  if $m \le a$ **then**
    $quotient \leftarrow quotient + (1 << i)$
    $a \leftarrow a - m$
  end if
end for
return $quotient$

算法1的复杂度为$\Theta(\beta^2)$，余数只需计算$a - b * quotient$即可，乘法需$\Theta(\beta^2)$，加法需$\Theta(\beta)$，因此也只需$\Theta(\beta^2)$.

31.1-13

Proof. 根据算法2和算法3，可以得到递推式：$T(\beta) = 2T(\frac{\beta}{2}) + M(\frac{\beta}{2})$，由主定理可知算法运行时间是$\Theta(M(\beta)\lg\beta)$. □

31.2-4

见算法4.

31.2-5

Proof. 由定理31.11可知，若k满足$b < F_{k+1} = \frac{\Phi^k}{\sqrt{5}}$，

Algorithm 2 BIT-CONVERT($\beta, a[], p, r, left, bit$)

if $p < r$ **then**
  $q \leftarrow (p + r)/2$
  BIT-CONVERT($a, p, q, 0, bit$)
  BIT-CONVERT($a, q + 1, r, 1, bit$)
end if
if $p \le r$ and $bit < \beta$ **then**
  if $left == 0$ **then**
    return BIT-MERGE(a, p, q, bit)
  end if
else
  return BIT-MERGE($a, q + 1, r, bit$)
end if

Algorithm 3 BIT-MERGE($a[], p, r, bit$)

$ret \rightarrow 0$
if $p \le bit$ **then**
  $p \leftarrow bit + 1$
end if
for $i \leftarrow p$ **to** r **do**
  $bit \leftarrow bit + 1$
  $ret \leftarrow ret + (a[i] << i)$
end for
return ret

Algorithm 4 EUCLID-ITERATIVE(a, b)

while $b > 0$ **do**
  $temp \leftarrow a$
  $a \leftarrow b$
  $b \leftarrow temp \mod b$
end while
return a

则EUCLID(a,b)的递归调用次数少于k次.对于$k=1+\log_\Phi b$来说，有$\frac{\Phi^k}{\sqrt{5}}=\frac{\Phi^{2+\log_\Phi b}}{\sqrt{5}}=\frac{b\cdot\Phi^2}{\sqrt{5}}$，由于$\frac{\Phi^2}{\sqrt{5}}=\frac{3\sqrt{5}+5}{10}>1$，因此$b<\frac{\Phi^k}{\sqrt{5}}$，所以EUCLID$(a,b)$至多执行$1+\log_\Phi b$次递归调用即可.

若把界改进为$1+\log_\Phi(b/\gcd(a,b))$，首先证明引理：如果$a>b\geq 1$并且EUCLID(a,b)执行了$k\geq 1$次递归调用，则$a\geq\gcd(a,b)F_{k+2},b\geq\gcd(a,b)F_{k+1}$.当$k=1$时，有$a\geq 2\gcd(a,b),b=\gcd(a,b)$.假设当$k-1$时成立，则当$k$时，第一个指令是EUCLID$(b,a\mod b)$，因此递归$k-1$次，所以有$b\geq\gcd(a,b)F_{k+1},a\mod b\geq\gcd(a,b)F_k$，于是$a\geq b+(a\mod b)\geq\gcd(a,b)(F_{k+1}+F_k)=\gcd(a,b)F_{k+2}$.于是得证.由此，当$k=1+\log_\Phi(b/\gcd(a,b))$时，即有$b\gcd(a,b)<F_{k+1}$，至多执行$k$步即可. □

31.2-6

因为

$$\gcd(F_{k+1},F_k)=\gcd(F_k,F_{k-1})$$

且

$$\gcd(F_{k+1},F_k)=1,\text{floor}(\frac{F_{k+1}}{F_k})=1$$

算法返回的d值必为1，下面讨论算法返回的x,y值.通过(F_4,F_3)返回$(1,F_1,-F_2)$，(F_5,F_4)返回$(1,-F_2,F_3)$可推测:
(F_{k+1},F_k)返回$(1,(-1)^{k+1}F_{k-2},(-1)^kF_{k-1})$.
假设在$k-1$的情况下成立，也即(F_k,F_{k-1})返回$(1,(-1)^kF_{k-1},(-1)^{k-1}F_{k-2})$，则在$k$的情况下，$(F_{k+1},F_k)$返回值为
$(1,(-1)^{k-1}F_{k-2},(-1)^kF_{k-3})$
$=(1,(-1)^{k-1}F_{k-2},(-1)^k(F_{k-3}+F_{k-2}))$
$=(1,(-1)^{k+1}F_{k-2},(-1)^kF_{k-1})$，得证.
综上所述，当$k=1$时返回$(1,0,1)$，当$k=2$时返回$(1,0,1)$，当$k\geq 3$时，返回$(1,(-1)^{k+1}F_{k-2},(-1)^kF_{k-1})$.

31.2-9

Proof. (1) 若n_1,n_2,n_3,n_4两两互质，则$\gcd(n_1,n_2)=1,\gcd(n_1,n_4)=1$，因此$\gcd(n_1,n_2n_4)=1$，同理可知$\gcd(n_3,n_2n_4)=1$，由此可得$\gcd(n_1n_3,n_2n_4)=1$，同理可证$\gcd(n_1n_2,n_3n_4)=1$.

(2) 若$\gcd(n_1n_2,n_3n_4)=\gcd(n_1n_3,n_2n_4)=1$，则存在$x,y\in\mathbb{Z}$，使得$n_1n_2x+n_3n_4y=1$，根据不同的结合如：$n_1(n_2x)+n_3(n_4y)=1,n_1(n_2x)+n_4(n_3y)=1$可依次推出$(n_1,n_3),(n_1,n_4),(n_2,n_3),(n_2,n_4)$互质，由另一个条件可推出$(n_1,n_2),(n_3,n_4)$互质，由此可知$n_1,n_2,n_3,n_4$两两互质.

(3) 由此证得充分必要性.

□

31.3-5

Proof. 为了证明函数f_a是$\mathbb{Z}_n^*$的一个置换，只要证明f_a是$\mathbb{Z}_n^*$到$\mathbb{Z}_n^*$的双射.首先像与原像的元素个数相同，故只要证明对于每一个$y\in\mathbb{Z}_n^*$都存在某$x\in\mathbb{Z}_n^*$使得$f_a(x)=y$.因为$\mathbb{Z}_n^*$是阿贝尔群，存在逆元，故$f_a(a^{-1}y)=aa^{-1}y\mod n=y\mod n=y$，由此可知$f_a$满足双射，所以函数$f_a$是$\mathbb{Z}_n^*$的一个置换. □

31.4-2

Proof. 因为$ax\equiv ay(\mod n)$，所以$a(x-y)\equiv 0(\mod n)$，又因为$\gcd(a,n)=1$，所以n整除a当且仅当$n=1$，此时显然有$x\equiv y(\mod 1)$.若$n\geq 2$，则因为n整除$(x-y)$，所以有$x\equiv y(\mod n)$，得证. □

反例：$a=2,n=6$，此时方程$2x\equiv 2y(\mod 6)$的一个解为$x=2,y=5$，然而$2\equiv 5(\mod 6)$是不成立的.因此条件$\gcd(a,n)=1$是必要的.

31.4-3

仍然能输出正确的结果

Proof.

$$ax_0\equiv a(x'(b/d)\mod (n/d)(\mod n)$$

$$\equiv a(x'(b/d)-t(n/d))(\mod n)$$

$$\equiv d\cdot b/d-n(t/d)(\mod n)$$

$$\equiv b(\mod n)$$

因此仍然可以得到原先的解集. □

31.5-2

由题意知，$x \equiv 1(\mod 9)$
$x \equiv 2(\mod 8)$
$x \equiv 3(\mod 7)$
由$c_1 = 56(5 \mod 9) = 280$
$c_2 = 63(7 \mod 8) = 441$
$c_3 = 72(4 \mod 7) = 288$
所以$a = 1 \cdot 280 + 2 \cdot 441 + 3 \cdot 288$，故$a \equiv 10(\mod 504)$，因此$a$的通解为$10 + 504k, k \in \mathbb{Z}$.

31.5-3

Proof. 由定理31.27的定义可知，欲证题中的对应关系成立，即证$(a^{-1} \mod n) \mod n_i = a_i^{-1} \mod n_i$，即证

$$a^{-1} \mod n \equiv a_i^{-1}(\mod n_i)$$

即证

$$aa^{-1} \mod n \equiv aa_i^{-1}(\mod n_i)$$

即证

$$a \equiv a_i(\mod n_i)$$

又因为$a_i = a \mod n_i$，所以即证

$$a \equiv a \mod n_i(\mod n_i)$$

这是显然的，因此得证. □

31.6-2

Algorithm 5 MODULAR-EXPO(a, b, n)

$d \leftarrow 1$
$t \leftarrow a$
let $\langle b_k, b_{k-1}, \cdots, b_0 \rangle$ be the binary representation of b
for $i \leftarrow 0$ **to** k **do**
  if $b_i == 1$ **then**
    $d \leftarrow t \cdot d \mod n$
  end if
  $t \leftarrow t \cdot t \mod n$
end for
return d

31.6-3

由欧拉定理可知$a^{\Phi(n)} \equiv 1(\mod n)$，则可知$a^{-1} \equiv a^{\Phi(n)-1}(\mod n)$，因此只需要调用MODULAR-EXPONENTIATION$(a, \Phi(n) - 1, n)$即可计算出$a^{-1} \mod n$.