第 4-5 讲: 数论算法

姓名： 林凡琪　　**学号：** 211240042

评分： ______　　**评阅：** ______

2023 年 3 月 29 日

请独立完成作业，不得抄袭。
若得到他人帮助, 请致谢。
若参考了其它资料，请给出引用。
鼓励讨论，但需独立书写解题过程。

1 作业 (必做部分)

题目 1 (TC 31.1-12)

解答:
基本思想：左移，直到两个数字长度相同，然后使用适当的乘数重复减去并向右移动。

Algorithm 1 DIVIDE

```
function DIVIDE(n)                          ▷ 通常伪代码的函数名是这样特殊的大写
    for i = β − α, 0 do
        while a[i, ..., i + α − 1] − b[0, ..., α − 1] ≥ 0 do
            a[i, ..., i + α − 1] −= b[0, ..., α − 1]
            c[i] + +
        end while
    end for
    d = a
    return c, d
end function
```

题目 2 (TC 31.2-5)

解答:
1. 当 b=0, 不进行递归
2. 当 b>1 根据 Lemma 31.10 可知：

$$\begin{aligned} b \geq F_{k+1} \approx \phi^{k+1}/\sqrt{5} &\Rightarrow \lg_\phi b \geq k+1-\lg_\phi \sqrt{5} \\ &\Rightarrow k+1 \leq \lg_\phi \sqrt{5} + \lg_\phi b \\ &\Rightarrow k+1 < 1.73 + \lg_\phi b \\ &\Rightarrow k < 1 + \lg_\phi b \end{aligned}$$

EUCILID(a,b) 和 EUCLID(a/gcd(a,b),b/gcd(a,b)) 的递归次数相同。

题目 3 (TC 31.3-5)

解答:
为了证明它是一个置换，我们需要证明对于 $\mathbb{Z}_n^*$ 中的每个元素 x，$f_a(x) \in \mathbb{Z}_n^*$，由 f_a 生成的数字是不同的。

因为 $a \in \mathbb{Z}_n^*$ 并且 $x \in \mathbb{Z}_n^*$, 那么 $f_a(x) = ax \mod n \in \mathbb{Z}_n^*$ （根据 closure property）
.

下面利用反证法：假设 $x, y \in \mathbb{Z}_n^*$，那么，$f_a(x) = f_a(y)$

$$\begin{aligned} f_a(x) &= f_a(y) \\ ax \mod n &= ay \bmod n \\ (a \mod n)(x \bmod n) &= \left(a \quad \bmod n \right)(y \bmod n) \\ (x \mod n) &= y \bmod n \\ x &\equiv y \bmod n \end{aligned}$$

和假设矛盾。

得证。

题目 4 (TC 31.4-2)

解答:

$$d = gcd(ax, n) = gcd(x, n)$$

因为 $ax \cdot x' + n \cdot y' = d$,

我们有

$$x \cdot (ax') + n \cdot y' = d.$$

$$\begin{aligned} x_0 =& x'(ay/d), \\ x_0' =& (ax')(y/d) = x'(ay/d) = x_0. \end{aligned}$$

题目 5 (TC 31.5-2)

解答:
应用中国剩余定理

$$n = 9 \times 8 \times 7 = 504$$

$$a_1 = 1, a_2 = 2, a_3 = 3$$

$$m_1 = 56, m_2 = 63, m_3 = 72$$

$$m_1^{-1} = 5 \bmod 9, m_2^{-1} = 7 \bmod 8, m_3^{-1} = 4 \bmod 7$$

$$\begin{aligned} c_1 = 280, c_2 &= 441, c_3 = 288 \\ x &\equiv 280 \times 1 + 441 \times 2 + 288 \times 3 \bmod 504 \\ &= 10 \bmod 504 \end{aligned}$$

题目 6 (TC 31.6-2)

解答：

```
MODULAR-EXPONENTIATION(a, b, n)
i = 0
d = 1
while (1 << i)    b
if (b & (1 << i)) > 0
d = (d * a) % n
a = (a * a) % n
i = i + 1
return d
```

题目 7 (TC 31.1-13(有勘误))

Give an efficient algorithm to convert a given β-bit (binary) integer to a decimal representation. Argue that if multiplication or division of integers whose length is at most β takes time $M(\beta) = \Omega(\beta)$, then we can convert binary to decimal in time $O(M(\beta)\lg\beta)$. (Hint: Use a divide-and-conquer approach, obtaining the top and bottom halves of the result with separate recursions.)

勘误详细参见：https://www.cs.dartmouth.edu/ thc/clrs-bugs/bugs-3e.php

解答：

预处理求出 $2^k(0 \le k \le \beta)$

分别递归求出左半段 L、右半段 R

$$F(X) = F(X.L) * 2^{LEN(X.R)} + F(X.R)$$

题目 8 (TC 31.2-9)

解答：

假设 $n_1 n_2 x + n_3 n_4 y = 1$，则 $n_1(n_2 x) + n_3(n_4 y) = 1$，因此 n_1 和 n_3 互质，n_1 和 n_4，n_2 和 n_3，n_2 和 n_4 都是互质的。由于 $\gcd(n_1 n_3, n_2 n_4) = 1$，所有这些数对都是互质的。

一般来说，第一轮将元素分成两组，每组元素的数量相等，分别计算两组的乘积，如果两个乘积互质，则一组中的元素与另一组中的元素成对互质。在下一轮迭代中，对于每个组，我们将元素分成两个子集，假设我们有子集 $(s_1, s_2), (s_3, s_4), \ldots$，然后我们计算 $s_1, s_3, \ldots$ 和 $s_2, s_4, \ldots$ 的乘积，如果这两个乘积互质，则所有子集对都成对互质，类似于第一轮。在每次迭代中，子集中的元素数量是原始集合的一半，因此有 $\lceil \lg k \rceil$ 对乘积。

为了有效地选择子集，在第 k 次迭代中，我们可以根据索引的第 k 位的值将数字分成两部分。

题目 9 (TC 31.5-3)

解答:
根据 TH 31.27
令 $b=a^{-1}$, 那么

$$b \leftrightarrow \left(b_1, b_2, \cdots, b_k\right), \text{ where } b_i = b \bmod n_i$$

只需要证明 $\forall i$:

$$\begin{aligned}
& a_i^{-1}=b_i=(b \bmod n) \bmod n_i \\
& =\left(a^{-1} \bmod n\right) \bmod n_i \\
& \operatorname{gcd}(a, n)=1 \quad \Rightarrow \operatorname{gcd}\left(a, n_i\right)=1 \\
& \Rightarrow \operatorname{gcd}\left(a \bmod n_i, n_i\right)=\operatorname{gcd}\left(a_i, n_i\right)=1 \\
& \Rightarrow a_i \cdot x \equiv 1 \bmod n_i \text{ 在模意义下存在唯一解, 记为} t .
\end{aligned}$$

因为, $t=a_i^{-1} \bmod n_i$. 并且 $a_i \cdot n_i\left(\left(a^{-1} \bmod n\right) \bmod n_i\right)=\left(a \bmod n_i\right) \cdot n_i\left(a^{-1} \bmod n_i\right)=1$ 所以, $a_i^{-1}=\left(a^{-1} \bmod n\right) \bmod n_i$

题目 10 (TC 31.6-3)

解答:

$$\begin{aligned}
a^{\phi(n)} & \equiv 1 && (\bmod n), \\
a \cdot a^{\phi(n)-1} & \equiv 1 && (\bmod n), \\
a^{-1} & \equiv a^{\phi(n)-1} && (\bmod n).
\end{aligned}$$

---

2 作业 (选做部分)

题目 1 (同余方程组)
解同余方程组:

$$\begin{aligned}
x & =3(\bmod 8), \\
x & =11(\bmod 20), \\
x & =1(\bmod 15).
\end{aligned}$$

解答:

---

3 Open Topics

Open Topics 1 (乘法算法)
请给出 n 位整数相乘的算法

- $O(n^2)$?

- $O(n^{\lg 3})$?
- 更快的其他算法?

(参考资料：https://en.wikipedia.org/wiki/Multiplication_algorithm)

Open Topics 2 (Pollard's rho algorithm)
Pollard's rho algorithm is an algorithm for integer factorization.

(参考资料：https://en.wikipedia.org/wiki/Pollard's_rho_algorithm)

4　反馈