第 4-5 讲: 数论算法

姓名： 朱宇博　　**学号：** 191220186

评分： ______　　**评阅：** ______

2021 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)

Algorithm 1 div

解答：

```
procedure DIV(A[1, ..., β], B[1, ..., α])        ▷ A is Dividend and B is divisor
    C[1...β] = 0
    for i ← β − α + 1 → 1 do
        while A[β, ..., i] ≥ B[α, ..., 1] do
            A[β, ..., i] ← A[β, ..., i] − B[α, ..., 1]
            C[i] ← C[i] + 1
        end while
    end for
    return A, C                                  ▷ A is remainder and C is quotient
end procedure
```

题目 2 (TC 31.2-5)

解答：

假设该算法执行了 k 次迭代，则由引理 3.10 可知，$b \geq F_{k+1}$，即 $b \geq \frac{\phi^{k+1}}{\sqrt{5}}$

从而得到 $k+1 \leq \log_\phi \sqrt{5} + \log_\phi b$, 推得 $k < 1 + \log_\phi b$

设整数 r 和 s 的最大公因数为 d, 根据欧几里得算法，$gcd(r, s)$ 调用一次后变成 $gcd(s, r \mod s)$, $gcd(rd, sd)$ 调用一次后变成 $gcd(sd, (r \mod s)d)$

根据算法终止条件，当第二维为 0 时停止递归。由于 $r \mod s = 0$ 当且仅当 $(r \mod s)d$ 为 0（d 不为 0）

故 $gcd(r,s)$ 和 $gcd(rd,sd)$ 迭代次数相同。
由此引理可知 $gcd(\frac{a}{gcd(a,b)}, \frac{b}{gcd(a,b)})$ 和 $gcd(a,b)$ 的次数相同。
将 $\frac{b}{gcd(a,b)}$ 代入，可得 $k < 1 + \log_\phi \frac{b}{gcd(a,b)}$

题目 3 (TC 31.3-5)

解答:
$\forall x_1, x_2 \in \mathbb{Z}_n^*, f_a(x_1) = f_a(x_2) \rightarrow ax_1 \mod n = ax_2 \mod n \rightarrow x_1 = x_2$(群的 right and left cancellation laws)
$\forall y \in \mathbb{Z}_n^*, \exists x = a^{-1}y \mod n \in \mathbb{Z}_n^*, f_a(x) = y$
因此 f 是双射函数，可得其为 $\mathbb{Z}_n^*$ 的一个置换

题目 4 (TC 31.4-2)

解答:
当 $gcd(a,n) = 1$ 时，a 存在逆元 a' 使得 $aa' \equiv 1 \pmod n$。则

$$ax \equiv ay \pmod n \rightarrow a'ax \equiv a'ay \pmod n \rightarrow x \equiv y \pmod n$$

当 $n = 4$ 时，$2 * 5 \equiv 2 * 3 \pmod 4$ 但 5 和 3 在模 4 的意义下不相等

题目 5 (TC 31.5-2)

解答:
$m_1 = 56, m_2 = 63, m_3 = 72, c_1 = 280, c_2 = 441, c_3 = 288$

$$\begin{aligned} a &\equiv 1 * c_1 + 2 * c_2 + 3 * c_3 \pmod{9 * 8 * 7} \\ &\equiv 2026 \pmod{504} \\ &\equiv 10 \pmod{504} \end{aligned}$$

题目 6 (TC 31.6-2)

Algorithm 2 quick-mod

解答:

procedure QUICK_MOD(a, b, n) ▷ $ab\%n$
  $ans \leftarrow 1$
  while $b \neq 0$ **do**
    if $b \mod 2 == 1$ **then**
      $ans \leftarrow ans * a\%n$
    end if
    $a \leftarrow a * a\%n$
    $b \leftarrow \lfloor \frac{b}{2} \rfloor$
  end while
  return ans
end procedure

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:

采用分治算法解决该问题，每次将二进制串分为两部分，分而治之，递归处理计算每部分转成十进制后的结果。
在合并时，将高位所在区间的结果，乘上对应位数的位权。根据题设已知乘法时间
故 $T(\beta) = 2T(\frac{\beta}{2}) + M(\beta)$，解得 $T(\beta) = O(M(\beta) \lg \beta)$

题目 8 (TC 31.2-9)

解答:

Theorem 31.6

For any integers a, b, and p, if both $gcd(a, p) = 1$ and $gcd(b, p) = 1$, then $gcd(ab, p) = 1$.

(1)

充分性:

若 $gcd(n_1n_2, n_3n_4) = 1$，即可推出 n_1, n_2 中任意整数，与 n_3 n_4 中任意整数互质。

证明: 反证。不失一般性地假设 $gcd(n_1, n_3) = k(k > 1)$，则 $k|gcd(n_1n_2, n_3n_4)$，与题设相悖。故得证。

同理，$gcd(n_1n_3, n_2n_4) = 1$，即可推出 n_1, n_3 中任意整数，与 n_2, n_4 中任意整数互质。

综上可得出 n_1, n_2, n_3, n_4 互质。即 $gcd(n_1n_2, n_3n_4) = 1 \wedge gcd(n_1n_3, n_2n_4) = 1 \rightarrow n_1, n_2, n_3, n_4$ 互质。

必要性:
若 n_1, n_2, n_3, n_4 互质, 由 TH31.6，可得 $gcd(n_1n_2, n_3) = 1, gcd(n_1n_2, n_4) = 1$, 再用 TH31.6，可得 $gcd(n_1n_2, n_3n_4) = 1$。同理，$gcd(n_1n_3, n_2n_4) = 1$。得证
故为充要条件。
(2)
充分性:
我们需要找到一种划分方法，使得经过 $\lceil\lg k\rceil$ 对互质条件后，推出每两个数之间互质。
为简便起见，以下讨论**不考虑奇偶对"均分"带来的影响**。
初始时，所有的数均标号为 1, 若要推出所有元素之间互质，我们需要证相同标号的数字之间互质。
第一次: 将原标号为 1 的数**均分**成两部分, 分别标号 1,2。则将 {标号为 1},{标号为 2} 作为新数对。显然这之后，我们仍只需证相同标号的元素之间互质。。
第二次：将原标号为 1 的数**均分**成两部分，分别标号 1,2。将原标号为 2 的数均分成两部分，分别标号 3,4。则将 {标号为 1 和 3},{标号为 2 和 4} 作为新数对。显然这之后，我们仍只需证相同标号的元素之间互质。
第 k 次：将原标号为 k 的数**均分**成两部分，分别标号 $2k-1$,$2k$。则将 {标号为奇数}, {标号为偶数} 作为新数对。显然这之后，我们仍只需证相同标号的元素之间互质。
当划分到每个标号都只有 1 个数时，即可说明两两互质。
因为标号相同的数在每一轮开始时，都会被**均分**成两组标号不同的数，故经过 $\lceil\lg k\rceil$ 次后，即可满足每个标号都只有 1 个数。
故我们找到了一种经过 $\lceil\lg k\rceil$ 对互质条件后，推出每两个数之间互质的方法。充分性得证。

必要性:
若 n_1, n_2, n_3, n_4 互质, 由 TH31.6 即其拓展，显然可得其中导出的 $\lceil\lg k\rceil$ 对整数互质。

题目 9 (TC 31.5-3)

解答:
由于 $gcd(n, a) = 1$，根据群的性质，在 $\mathbb{Z}_n$ 中，有

$$a^{-1} \leftrightarrow a$$

由中国剩余定理，有

$$a \leftrightarrow (a_1, a_2, ..., a_n)$$

由于 $gcd(n, a) = 1$，可推得 $gcd(n_i, a) = 1$。
由欧几里得定理,$gcd(n_i, a_i) = gcd(n_i, a \mod n_i) = gcd(n_i, a) = 1$。
根据群的性质，在 $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times ... \times \mathbb{Z}_{n_k}$ 中，有

$$(a_1, a_2, ..., a_k) \leftrightarrow (a_1^{-1}, a_2^{-1}, ..., a_k^{-1})$$

由以上三组关系的传递性，可得

$$a^{-1} \leftrightarrow (a_1^{-1}, a_2^{-1}, ..., a_k^{-1})$$

即

$$a^{-1} \mod n \leftrightarrow (a_1^{-1} \mod n_1, a_2^{-1} \mod n_2, ..., a_k^{-1} \mod n_k)$$

得证。

题目 10 (TC 31.6-3)

解答：
由欧拉定理，利用该算法计算 $a^{\phi(n)-1} \mod n$ 即可，该数即为 a 的模 n 乘法逆元。

---

2 作业（选做部分）

题目 1 (同余方程组)
解同余方程组：

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

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