※ 5.3 The Euclidean Algorithm

- Def: Algorithm for finding the greatest common divisor of two integer.

- Base: If $a \bmod b = r$, then $\gcd(a,b) = \gcd(b,r)$

  ↳ pf) There exist q and r satisfying $a=bq+r$ $(0 \le r < b)$

  Let c be a common divisor of a and b.

  So, $c \mid b$, then $c \mid bq$

  Thus $c \mid a$ and $c \mid bq$, then $c \mid (a-bq) = c \mid r$

  ⇒ c is common divisor b and r

ex) Find $\gcd(504, 396)$

① $504 \bmod 396 = 108$

② $396 \bmod 108 = 72$

③ $108 \bmod 72 = 36$

④ $72 \bmod 36 = 0$

$\gcd(a,b)=\gcd(b,r)$

∴ $\gcd(504, 396) = 36$

TABLE 5.3.2 ■ Smallest Input Pair That Requires n Modulus Operations in the Euclidean Algorithm

a	b	n (= number of modulus operations)
1	0	0
2	1	1
3	2	2
5	3	3
8	5	4
13	8	5

*1 $a \ge f_{n+2}$, $b \ge f_{n+1}$

where $\{f_n\}$ denotes the Fibonacci sequence

*2 ⇒ $\log_{3/2} \frac{2m}{3}$ modulus operation are required.

(integer in the range 0 to m, $m \ge 8$)

↳ pf*1 by induction

i) $n=1$, true

ii) $n=k+1$.

Suppose that the pair a, b, $a>b$, requires $n+1$ mod operations when input to algorithm.

$a = bq + r$ $(r = a \bmod b,\ 0 \le r < b)$

Using the values b and r.

$b \ge f_{n+2}$ and $r \ge f_{n+1}$ (n: additional mod operations)

Thus $a = bq + r$

$\ge b + r$

$\ge f_{n+2} + f_{n+1} = f_{n+3}$

⇒ $a \ge f_{n+3}$, $b \ge f_{n+2}$

pf)*2 Let n be the maximum number of mod operations required by the Euclidean algorithm for integers in the range 0 to m, $m \ge 8$.

Let a, b be an input integer (range 0 to m)

TABLE 5.3.1 ■ Number of Modulus Operations Required by the Euclidean Algorithm for Various Values of the Input

a \ b	0	1	2	3	4	5	6	7	8	9	10	11	12	13
0	—	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	1	1	1	1	1	1	1	1	1	1	1	1
2	0	1	1	2	1	2	1	2	1	2	1	2	1	2
3	0	1	2	1	2	3	1	2	3	1	2	3	1	2
4	0	1	1	2	1	2	2	3	1	2	2	3	1	2
5	0	1	2	3	2	1	2	3	4	3	1	2	3	4
6	0	1	1	1	2	2	1	2	2	2	3	3	1	2
7	0	1	2	2	3	3	2	1	2	3	3	4	4	3
8	0	1	1	3	1	4	2	2	1	2	2	4	2	5
9	0	1	2	1	2	3	2	3	2	1	2	3	2	3
10	0	1	1	2	2	1	3	3	2	2	1	2	2	3
11	0	1	2	3	3	2	3	4	4	3	2	1	2	3
12	0	1	1	1	1	3	1	4	2	2	2	2	1	2
13	0	1	2	2	2	4	2	3	5	3	3	3	2	1

$n \ge 4$ and that $a \ne b$ $(a>b)$

By *1, $a \ge f_{n+2}$ → $m \ge f_{n+2}$

→ $\left(\frac{3}{2}\right)^{n+1} < f_{n+2}$

$f_{n+2} = f_{n+1} + f_n$

$> \left(\frac{3}{2}\right)^{n} + \left(\frac{3}{2}\right)^{n-1}$

$> \left(\frac{3}{2}\right)^{n+1} \cdot \frac{10}{9}$

$> \left(\frac{3}{2}\right)^{n+1}$

⇒ $\left(\frac{3}{2}\right)^{n+1} < m$

$n+1 < \log_{3/2} m$

∴ $n < \log_{3/2} m - 1 = \log_{3/2} \frac{2}{3}m$

- Extended Euclidean Algorithm

  - Let $a>0$, $b>0$ be integer. There exist integers s and t such that $\gcd(a,b) = sa + tb$

  - It can be used to find the solution that satisfied with indeterminate equation $ax+by=c$

    ↳ minimum of c is $\gcd(a,b)$

ex) $\gcd(273, 110)$

1. find the gcd

$273 \bmod 110 = 53$

$110 \bmod 53 = 4$

$53 \bmod 4 = 1$

$4 \bmod 1 = 0$

2. find the s,t

$1 = 53 - 4 \cdot 13$

$4 = 110 - 53 \cdot 2$

→ $1 = 53 - (110 - 53 \cdot 2) \cdot 13$

$= 27 \cdot 53 - 13 \cdot 110$

$53 = 273 - 110 \cdot 2$

→ $1 = 27 \cdot (273 - 110 \cdot 2) - 13 \cdot 110$

$= 27 \cdot 273 - 67 \cdot 110$

⇒ $\gcd(273, 110) = 1 = s \cdot 273 + t \cdot 110$

pf) Given $a > b \geq 0$. $r_0 = a$. $r_1 = b$

$r_{i+1} = r_{i-1} - q_i r_i$ $\because q_i = \frac{r_{i-1}}{r_i}$

If $r_{i+1} = 0$. then $gcd(a, b) = r_i$

① Initial condition: $s_1 = 1$. $s_2 = 0$. $t_1 = 0$. $t_2 = 1$.

$as_i + bt_i = r_i$ for $i = 0, 1$

② $i > 1$

$r_{i+1} = r_{i-1} - r_i q_i$

$= (as_{i-1} + bt_{i-1}) - (as_i + bt_i) q_i$

$= a(s_{i-1} - s_i q_i) + b(t_{i-1} - t_i q_i)$

$= as_{i+1} + bt_{i+1}$

If $r_{i+1} = 0$, then $as_i + bt_i = r_i$ is

$sa + tb = gcd(a, b)$

- Computing an Inverse Modulo an Integer

- Def: Let $n > 0$, $\phi > 0$ such that $gcd(n, \phi) = 1$,

  * $0 < s < \phi$ such that $ns \bmod \phi = 1$. We call s the inverse of $n \bmod \phi$.

  → There is no division operation in modular operation.

  ↳ $A^{-1} = A \bmod C$

  $A \cdot A^{-1} \equiv 1 \bmod C$

  $(A \cdot A^{-1}) \bmod C = 1$

pf) Let $n > 0$. $\phi > 0$ such that $gcd(n, \phi) = 1$,

using the Euclidean algorithm, find the s' and t' such that $s'n + t'\phi = 1$.

Then $ns' = -t'\phi + 1$ (1 is remainder)

$ns' \bmod \phi = 1$

Now that s' is almost the custom value. but s' may not satisfy $0 < s' < \phi$.

However convert s' to $s = s' \bmod \phi$

$(0 \leq s < \phi)$

Thus there exists q such that $s' = q\phi + s$

$ns = ns' - \phi n q = -t'\phi + 1 - \phi n q$

$= \phi(-t - nq) + 1$

- Step about finding the modular inverse

① $A \bmod C$

1. Calculate the $A \cdot B \bmod C$ about B from 0 to $C-1$

2. The inverse of modular of $A \bmod C$ is the B such that $A \cdot B \bmod C = 1$

ex) Find the inverse modular $3 \bmod 7$

1. $3 \cdot 0 \bmod 7 = 0$

   $3 \cdot 1 \bmod 7 = 1$

   ⋮ ⋮

   $3 \cdot 5 \bmod 7 = 1$

2. $B = 5$

② $ns \bmod \phi = 1$

1. Find the s', t' such that $s'n + t'\phi = 1$

2. Change the s' to $s = s' \bmod \phi$

ex) Let $n = 110$, $\phi = 273$. Find the s such that $s'n + t\phi = 1$.

1. Find the s', t'

   from extended euclidean algorithm example, we get the $s' = -67$, $t' = 27$

2. $110 \cdot (-67) \bmod 273 = 110 \cdot s \bmod 273$

   $= 1$

   $s = s' \bmod \phi = -67 \bmod 273$

   $= 206$

To calculate the minus modular

— Suppose $-a \bmod b$ $(a > 0, b > 0)$.

① $a \bmod b = \boxed{}$

② $-\boxed{} + b$