作業二 參考解答 繳交日期 112/03/16 (四) 15:10 請上傳 tronclass

1. (a) Find 12^{-1} (mod 1729) (b) Calculate by hand the solution of equation 12 x ≡ 1124 (mod 1729). (Please write out the process of calculation.)

Sol:

(a) $1729 = 144 \cdot 12 + 1$

$1 = 1729 \cdot 1 + 12 \cdot (-144)$

$12^{-1} \equiv -144 \pmod{1729} \equiv$ **1585** (mod 1729)

(b) gcd(12, 1729) = 1

$12^{-1} \cdot 12\,x \equiv 12^{-1} \cdot 1124 \pmod{1729}$

$x \equiv 1585 \cdot 1124 \pmod{1729} \equiv$ **670** (mod 1729)

2. The Fibonacci numbers are defined by $F_0 = 0, F_1 = 1, F_n = F_{n-1} + F_{n-2}$. (a) Show that if the quotients q_i (let $a \geq b, a = q_0 b + r_0, b = q_1 r_0 + r_1, r_0 = q_2 r_1 + r_2, \ldots$) appearing in the Euclidean algorithm for finding out gcd(a,b) are equal to one then a and b are consecutive Fibonacci numbers, (b) Show that the complexity of the Euclidean algorithm for finding gcd(a,b), a ≥ b, is O($\log_{10}$ b) integer divisions. (Asymptotically, integer division has the same complexity as integer multiplication, i.e. O($\log^2$n). Thus, the complexity of Euclidean algorithm is close to an exponentiation.)

Sol:

(a) Assume that for a pair (a, b), the Euclidean algorithm performs that following integer divisions and finds that all quotients are 1, $r_{n-3} = 2$, and gcd(a, b)=1

$a = 1 \cdot b + r_0$

$b = 1 \cdot r_0 + r_1$

$r_0 = 1 \cdot r_1 + r_2$

$r_1 = 1 \cdot r_2 + r_3$

…

$r_{n-4} = 1 \cdot r_{n-3} + 1$

Then $F_2 = 1$, $F_3 = r_{n-3} = 2$, $F_4 = r_{n-4}$, …, $F_n = r_0$, $F_{n+1} = b$, $F_{n+2} = a$ are the Fibonacci numbers. For example, (a, b) = (F_8, F_7) = (21, 13).

(b) The Euclidean algorithm performs worst (in terms of number of steps) for those bad pairs (a, b) which lead to all q_i=1 in the execution of the algorithm. Assume that the Euclidean algorithm terminates in N steps for a bad pair (a, b): for example N=5, we have the following

$a = b + r_0$

$b = r_0 + r_1$

$r_0 = r_1 + r_2$

$r_1 = r_2 + r_3$

$r_2 = r_3 + 1$

we then have the Fibonacci sequence $F_2 = 1$, $F_3 = r_3 = 2$, $F_4 = r_2$, …, $F_6 = b$, $F_7 = a$. In general we have

$b = F_{N+1}$ for a bad pair (a, b). Before we estimate the complexity of the algorithm, we need to have the following lemma

Lemma: If the Euclidean algorithm requires N steps for a pair (a, b), a≥b, then a and b must satisfy $a \geq F_{N+2}$ and $b \geq F_{N+1}$.

This can be proved by induction.

For N=1, $a = q_0 b+0$, b divides a with no remainder, the smallest natural numbers for this is b=1 and a=2, which are F_2 and F_3 respectively.

Assume that the result holds for all values of N up to M-1.

Consider N=M, the first step of the M-step algorithm is $a=q_0 b+r_0$, and the Euclidean algorithm requires M-1 additional steps for the pair (b, r_0) where $b>r_0$. By induction hypothesis, $b \geq F_{M+1}$ and $r_0 \geq F_M$. Therefore, $a=q_0 b+r_0 \geq b+r_0 \geq F_{M+1}+F_M = F_{M+2}$, which is the desired inequality

If the algorithm requires N steps, then b is greater than or equal to F_{N+1} which in turn is greater than or equal to φ^{N-1}, where φ is the golden ratio ($\varphi = \frac{1+\sqrt{5}}{2} = 1.618033988749$ ...). Since $b \geq \varphi^{N-1}$, then

$N-1 \leq \log_\varphi b$. Since $\log_{10}\varphi > 1/5$, $(N-1)/5 < \log_{10}\varphi \;\; \log_\varphi b = \log_{10} b$. Thus, $N \leq 5\log_{10} b$ and the complexity is $O(\log_{10} b)$ integer divisions.

3. Solve by hand the x's that satisfy the following system of congruence equations: (Please write out the process of calculation.)

$$\begin{cases} 7x \equiv 4 \pmod{93} \\ 15x \equiv 24 \pmod{39} \end{cases}$$

Sol:

Step 1. Solve x that satisfies $7 \cdot x \equiv 4 \pmod{93}$

1. gcd(7, 93)=1 implies that these is only one x that satisfies $7 \cdot x \equiv 4 \pmod{93}$
2. Find $7^{-1} \pmod{93}$ (formally by extended Euclidean algorithm) or (manually) $93 \equiv \mathbf{2} \pmod 7$, $\mathbf{2}^{-1} \equiv \mathbf{4} \pmod 7$, $1 = 7 \cdot s + 93 \cdot \mathbf{4}$, $s = (1-93)/7= -53$, i.e. $7^{-1} \equiv \mathbf{40} \pmod{93}$
3. $40 \cdot 7 \cdot x \equiv 40 \cdot 4 \pmod{93}$, i.e. the first congruence becomes $x \equiv 40 \cdot 4 \equiv \mathbf{67} \pmod{93}$ … ❶

Step 2. Solve x's that satisfy $15 \cdot x \equiv 24 \pmod{39}$

1. gcd(15,39)=3 and 3 | 24 imply that there are 3 x's that satisfy $15 \cdot x \equiv 24 \pmod{39}$
2. divide both sides by 3 and get the congruence equation $5 \cdot x \equiv 8 \pmod{13}$
3. gcd(5,13)=1 implies that only one x satisfies $5 \cdot x \equiv 8 \pmod{13}$
4. Find $5^{-1} \pmod{13}$ by enumerating 2,3,…,12, and find that $5^{-1} \equiv 8 \pmod{13}$
5. The solution to $5 \cdot x \equiv 8 \pmod{13}$ is $x \equiv 5^{-1} \cdot 8 \equiv 8 \cdot 8 \equiv 64 \equiv \mathbf{12} \pmod{13}$ **12** is also a solution to $15 \cdot x \equiv 24 \pmod{39}$
6. The other two solutions to $15 \cdot x \equiv 24 \pmod{39}$ are $12+13 = \mathbf{25}$, $12+13 \cdot 2 = \mathbf{38}$
7. Now the second congruence relation becomes $x \equiv 12$ or 25 or $38 \pmod{39}$ … ❷
8. Since $x \equiv 67 \pmod{93} \Leftrightarrow 67 \equiv 1 \pmod 3$ and $67 \equiv 5 \pmod{31}$ by CRT, we check $12 \equiv 0 \pmod 3$, $25 \equiv 1 \pmod 3$, $38 \equiv 2 \pmod 3$, Thus, the only one x that satisfy equations ❶ and ❷ is 25 and the congruence relations are equivalent to

$$\begin{cases} x \equiv 67 \pmod{93} \\ x \equiv 25 \pmod{39} \end{cases}$$

Step 3. Use CRT to solve the following system of congruence equations

Since gcd(93, 39) = 3, we need to decompose the above equations as

$x \equiv 1 \pmod{3} \equiv 12 \pmod{13} \equiv 5 \pmod{31}$

$m = 3 \cdot 13 \cdot 31 = 1209$

$m_1=3$,	$m_2=13$,	$m_3=31$
$r_1=1$,	$r_2=12$,	$r_3=5$
$z_1=403$,	$z_2=93$,	$z_3=39$
$s_1 \equiv 403^{-1} \equiv 1 \pmod{3}$,	$s_2 \equiv 93^{-1} \equiv 7 \pmod{13}$,	$s_3 \equiv 39^{-1} \equiv 4 \pmod{31}$

$x = z_1 \cdot s_1 \cdot r_1 + z_2 \cdot s_2 \cdot r_2 + z_3 \cdot s_3 \cdot r_3 \pmod{m}$

$= 403 \cdot 1 \cdot 1 + 93 \cdot 7 \cdot 12 + 39 \cdot 4 \cdot 5 \pmod{1209}$

$=$ **532** (mod 1209)

You can also solve the above system of 3 congruence relations progressively, i.e. first solve

$x \equiv 1 \pmod{3} \equiv 5 \pmod{31}$

which lead to the equivalent congruence relation $x \equiv 67 \pmod{93}$ and add the remaining congruence

$x \equiv 67 \pmod{93} \equiv 12 \pmod{13}$

find s and t satisfying 93 s + 13 t = 1,

s is $93^{-1} \pmod{13} \equiv 2^{-1} \pmod{13}$, enumerating 1,2, …, 12 and get 7

i.e. $93 \cdot 7 + 13\,t = 1$, therefore $t = (1-93\cdot 7)/13 = -50$

$x = 12\cdot 93\cdot 7 + 67\cdot 13\cdot(-50) = -35738 \equiv$ **532** (mod 1209)