Cryptography HW1

0716074蔡昌星

#1

$\mathbb{Z}_7$	乘反
$x_1 \equiv 1 \pmod 7$	1
$x_2 \equiv 2 \pmod 7$	4
$x_3 \equiv 3 \pmod 7$	5
$x_4 \equiv 4 \pmod 7$	2
$x_5 \equiv 5 \pmod 7$	3
$x_6 \equiv 6 \pmod 7$	6

#4 Euler's thm

$\phi(93) = 93 \times \frac{30}{31} \times \frac{2}{3} = 60$.

$7^{60} \equiv 1 \bmod 93$

$\Rightarrow (7^{60})^{16} \cdot 7^{53} \equiv 7^{53} \bmod 93$

$7^6 \equiv 4 \bmod 93$

$\Rightarrow (7^6)^8 \cdot 7^5 \pmod{93} = 4^8 \cdot 7^5 \bmod 93 = 10$ #

#5

$\phi(10) = 10 \times \frac{1}{2} \times \frac{4}{5} = 4$

$9^4 \bmod 10 = 1$

$9^{101} \bmod 10 = (9^4)^{25} \cdot 9 \bmod 10 = 9$ #

#2 $m = qn + r$, $q \geq 1$, $0 \leq r \leq n$, show "$\frac{m}{2} > r$".

(a) Assume that $\frac{m}{2} \leq r \Rightarrow m \leq 2r$

$m = qn + r \leq 2r \Rightarrow qn \leq r \Rightarrow q \leq \frac{r}{n} \leq 1$

$(\because r \leq n \Rightarrow \frac{r}{n} \leq 1$ and that $q \geq 1)$ ✗

by contradiction, the original proposition is correct. #

(b) $a_j = b_i \cdot q_i + r_i$

$b_i = r_i q_{i+1} + r_{i+1}$ ↓ 2 operation

$r_i = \cdots$

$r_i = a_{i+2}$

from the result of (a), $\frac{a_i}{2} > r_i = a_{i+2}$

$\therefore a_{i+2} < \frac{a_i}{2}$ #

(c) $m, n, N \in \mathbb{Z}$ $(1 \leq m, n \leq 2^N)$

by Euclidean algorithm, we should find m or n to be 0, then we can find gcd

Assume that we need k steps to find gcd, and from the result of (b): $a_{i+2} < \frac{a_i}{2}$

so m, n at least $2^{\frac{k}{2}}$, that is $m, n \geq 2^{\frac{k}{2}}$, compare to the question,

we get $\frac{k}{2} = N \Rightarrow k = 2N$ #

#3

(a)

	135, 1	61, 0	
2	122, 0	52, 4	4
	13, 1	9, −4	
1	9, −4	8, 10	2
	4, 5	1	−14

$1 = 135 \times (-14) + 61 \times 31$

$135 \times (-14) \equiv 1 \pmod{61}$

$\therefore x \equiv -14 \pmod{61}$ is the multiplicative inverse of 135 #

(b)

	7465, 1	2464, 0	
3	7392, 0	2409, 33	33
	73, 1	55, −33	
1	55, −33	54, 102	3
	18, 34	1	−135

$1 = 7465 \times -129 + 2464 \times 409$

$\Rightarrow 7465 \times -129 \equiv 1 \pmod{2464}$

$\therefore x \equiv -129 \pmod{2464}$ is the multiplicative inverse of 7465 #