Assignment 7

Problem 1 (4.18)

Let $n, b \in \mathbb{Z}$ with $0 \le b < n$, and let $EEA(n,b) = \{(r_i, s_i, t_i)\}_{i=0}^{\lambda+1}$.

This exercise develops some key properties of the fraction $-s_i/t_i$ as approximations to b/n. For $i = 1, \dots, \lambda+1$, let $\varepsilon_i := b/n + s_i/t_i$

(a) Show that $\varepsilon_i = r_i/t_i n$ for $i = 1, \dots, \lambda+1$

From EEA, we get $r_i = bt_i \pmod n$, $0 \le r < r_i$ and $0 < |t| < t^*$ / and

$s_{i+1} = s_{i-1} - s_i \times r_i$, $t_{i+1} = t_{i-1} - t_i \times r_i$

$\varepsilon_i = b/n + s_i/t_i$ $\quad b = r_1, n = r_0$ and $r_1 = bt_i \mod n$ so

$= b = bt_i \pmod n$ $\therefore t_1 = 1$. we also know that $t_0 = 0$, $s_0 = 1$, $s_1 = 0$

$\varepsilon_i = \frac{b}{n} + \frac{s_i}{t_i}$. Let's simplify this $\frac{b}{n} + \frac{s_i}{t_i} = \frac{bt_i + s_i n}{t_i n} = \frac{r_i}{t_i n} = r_i/t_i n$

we know $r_i = bt_i + ns_i$ so after simplify $\varepsilon_i = b/n + s_i/t_i = r_i/t_i n$

(b) Show that successive ε_i's strictly decrease in absolute value, and alternate in sign.

from $\varepsilon_i = r_i/t_i n$ we know n is fixed. From theorem 4.3 → "(iv) for $i = 0, \dots, \lambda$ we have $t_i t_{i+1} \le 0$ and $|t_i| \le |t_{i+1}|$; for $i = 1 \dots, \lambda$, we have $s_i s_{i+1} \le 0$ and $|s_i| \le |s_{i+1}|$;"

From this definition, we know t_i, s_i gets bigger as i increases and $t_i t_{i+1} \le 0$, so we know t_i changes sign alternatively as i increases. As r_i decrease as i increases, t_i increases as i increases. ε_i decrease in absolute valle and alternate in sign

(c) Show that $|\varepsilon_i| < 1/t_i^2$ for $i = 1, \ldots, \lambda$, and $\varepsilon_{\lambda+1} = 0$.

Let's say $|\varepsilon_i| \geq \frac{1}{t^2}$ then $\left|\frac{r_i}{t_i n}\right| \geq \frac{1}{t_i^2} \Rightarrow \left|\frac{r_i}{n}\right| \geq \frac{1}{|t_i|}$ and we know

$r_i = bt_i \pmod{n}$ so $\left|\frac{bt_i}{n}\right| \geq \frac{1}{|t_i|} \Rightarrow \left|\frac{b}{n}\right| \geq 1$ However n is bigger than

b so $\frac{b}{n}$ is smaller than 1. This is a contradition so $|\varepsilon_i| < \frac{1}{t_i^2}$

when $i = \lambda+1$ $r_{\lambda+1} = 0$ so $\varepsilon_{\lambda+1} = \frac{r_{\lambda+1}}{t_i n} = \frac{0}{t_i n}$ which is 0

(d) Show that for all $s, t \in \mathbb{Z}$ with $t \neq 0$, if $|b/n - s/t| < 1/2t^2$, then $s/t = -s_i/t_i$ for some $i = 1, \ldots, \lambda+1$. Hint use part (ii) of Theorem 4.9

Theorem 4.9 is " Let $n, b, r^*, t^* \in \mathbb{Z}$ with $0 \leq b < n$, $0 \leq r^* < n$, and $t^* > 0$. Further, let $EEA(n, b) = \{(r_i, s_i, t_i)\}_{i=0}^{\lambda+1}$, and let j be the smallest index $(0 \leq j \leq \lambda+1)$ such that $r_j \leq r^*$, and set

$$r' = r_j, \quad s' = s_j, \text{ and } t' = t_j$$

Finally, suppose that there exists $r, s, t \in \mathbb{Z}$ such that

$$r = ns + bt, \quad |r| \leq r^*, \text{ and } 0 < |t| \leq t^*$$

Then we have:

(i) $0 < |t'| \leq t^*$

(ii) if $n > 2r^*t^*$, then for some non-zero integer q,

$$r = r'q, \quad s = s'q, \text{ and } t = t'q.$$

$|b/n - s/t| < 1/2t^2 \Rightarrow 2t^2 \times \left|\frac{b}{n} - \frac{s}{t}\right| < \frac{1}{2t^2} \times 2t^2 = \left|\frac{2t^2 b}{n} - 2ts\right| < 1$

$\Rightarrow \left|\frac{2t^2 b - 2tsn}{n}\right| < 1 \Rightarrow \left|\frac{-2t(ns + tb)}{n}\right| < 1 \Rightarrow \left|\frac{-2tr}{n}\right| < 1$

$\Rightarrow |-2tr| < n$ so we know $n \geq |tr|$ so for some non-zero integer q, $r' = r'q$, $s = s'q$, and $t = t'q$. so $\frac{s}{t} = \frac{s'q}{t'q} = \frac{s'}{t'}$ for some $i = 1, \ldots, \lambda+1$

(e) consider a fixed index $i \in \{2, .., z+1\}$. Show that for all $s, t \in \mathbb{Z}$, if $0 < |t| \leq |t_i|$ and $|b/n - s/t| \leq |\varepsilon_i|$, then $s/t = -s_i/t_i$. In this sense, $-s_i/t_i$ is te unique, best approximation to b/n among all fractions of denominaton at most $|t_i|$. Hint: use part (i) of Theorem 4.9.

we have $0 < |t| \leq |t_i|$ and $|b/n - s/t| \leq |\varepsilon_i|$ which is

$|b/n - s/t| \leq |\frac{b}{n} + \frac{s_i}{t_i}|$ so we know $|-\frac{s}{t_i}| \leq |\frac{s_i}{t_i}|$ for all $s, t \in \mathbb{Z}$

so $\frac{s_i}{t_i}$ is unique then $\frac{s}{t} = -\frac{s_i}{t_i}$

Problem 2 (4.26)

To speed up RSA encryption, one may choose a very small encryption exponent. This exercise develops a "small encryption exponent attack" on RSA. Suppose Bob, Bill, and Betty have RSA public keys with moduli n_1, n_2, and n_3, and all three use encryption exponent 3. Assume that $\{n_i\}_{i=1}^{3}$ is pairwise relatively prime. Suppose that Alice encodes her message as an integer a, with $0 \leq a < \min\{n_1, n_2, n_3\}$, and computes the three encrypted messages $\beta_i := [a^3]_{n_i}$, for $i = 1, \dots, 3$. Show how to recover Alice's message from these three encrypted messages.

When Alice encrypt her messages to Bob, Bill, and Betty she has her pairwise public keys n_1, n_2, n_3 for Bob, Bill, and Betty with exponet $e=3$. We know n_1, n_2, and n_3 are relatively prime to each others and they should also relatively prime to 3. ($\gcd(3, \varphi(n_1)) = \gcd(3, \varphi(n_2)) = \gcd(3, \varphi(n_3)) = 1$)

We have encrypted message m from Alice's message a to each person, $[a^3]_{n_1}$, $[a^3]_{n_2}$, $[a^3]_{n_3}$.

Bob, Bill, and Betty have each their own private key d_1, d_2, and d_3 ($d_1 = 3^{-1} \bmod n_1$, $d_2 = 3^{-1} \bmod n_2$, $d_3 = 3^{-1} \bmod n_3$)

So in order to decrypte each messge,

For Bob first $m_1 = a^3 \bmod n_1$ $\quad m_1^{d_1} = (a^3)^{3^{-1}} \bmod n_1 = a^{3 \times 3^{-1}} \bmod n_1$

$= a^{\varphi(n_1) \times k + 1} \bmod n_1$ for some integer $k \in \mathbb{Z}$.

$= a \times a^{\varphi(n_1) \times k} \bmod n_1 = a \times a^{(p_1-1)(q_1-1) \times k} \bmod (p_1 \times q_1)$, $n_1 = p_1 q_1$ (each prime)

$= a \times (a^{(p_1-1)})^{(q_1-1) \times k} \bmod p_1$

$= a \cdot 1^{(q_1-1) \cdot k} \bmod p_1$

$= a$

This allies to Bill and Betty the same so we can decrypt Alice's message in the same way.