Algorithms - Ex13 Solutions

1 Question 1:

- We would like to prove that $<a>=<b>=\{0, d, 2d, \ldots, (\frac{n}{d}-1)d\}$. First we show that $d \in <a>$. Extended-Euclid gives us integers x' and y' such that $ax'+ny'=d$. This means that $ax' \equiv d \ (mod\, n)$ and therefore $d \in <a>$. Since $d \in <a>$, then every multiple of d is in $<a>$, and thus $<d> \subset <a>$.

  In the other direction, let $m \in <a>$. Then $m = ax+ny$ for some integers x, y. $d|a$ and $d|n$, so $d|ax+ny=m$, and therefore $m \in <d>$.

- To prove that $gcd(a,n)|b \Rightarrow ax \equiv b \ (mod\ n)$ has a solution, Let $d = gcd(a,n)$. If $d|b$ then $b \in <d>$, and by the previous section, $b \in <a>$, and therefore there exist x, y such that $ax+ny=b$, and x is a solution to the equation.

  To prove that $ax \equiv b \ (mod\ n)$ has a solution $\Rightarrow \ gcd(a,n)|b$, notice that if there is a solution to the equation this means that there exist integers x, y such that $ax+ny=b$. Since $gcd(a,n)|a$ and $gcd(a,n)|n$, $gcd(a,n)|ax+ny=b$.

- Obviously $a\frac{n}{d} \equiv 0 \ (mod\, n)$, since $\frac{a}{d}$ is an integer. So we know that the sequence $ak \ (mod\, n)$ has a period of $\frac{n}{d}$. It cannot have any smaller period since if there is a period h with $h < \frac{n}{d}$ then $<a> = \{ak \ (mod\, n)|k = 0, \ldots, n-1\}$ has only h elements, in contradiction to what we proved in the first section.

- The first $\frac{n}{d}$ elements of the sequence $ak \ (mod\, n)$, $k = 0, \ldots, n-1$ are exactly the elements of $<a>$, and since we proved that this sequence has a period of $\frac{n}{d}$, each element of $<a>$ is repeated exactly d times in the sequence. If $ax \equiv b \ (mod\, n)$ has a solution then $b \in <a>$, therefore it appears d times in the sequence, which means that there exist $k_1, \ldots, k_d$ such that $ak_i \equiv b \ (mod\, n)$ for $i = 1, \ldots, d$.

- We know that $ax' \equiv d \ (mod\, n)$, and therefore

  $$ax'\frac{b}{d} \equiv d\frac{b}{d} \ (mod\, n)$$

  $$\equiv b \ (mod\, n)$$

  which proves that $x'\frac{b}{d} \ (mod\, n)$ is a solution to the modular equation.

- The rest of the solutions of this modular equation are $x'\frac{b}{d} + i\frac{n}{d}$ for $i = 1, \ldots, d-1$. These are all distinct since $0 \leq i\frac{n}{d} < n$ for $i = 0, \ldots, d-1$, and for every $i > 0$ we have

  $$a(x'\frac{b}{d} + i\frac{n}{d}) \equiv ax'\frac{b}{d} + ai\frac{n}{d} \equiv b \ (mod\, n)$$

  (we already proved that $ax'\frac{b}{d} \equiv b \ (mod\, n)$, and $ai\frac{n}{d} \equiv 0 \ (mod\, n)$ since $\frac{ai}{d}$ is an integer).

- An algorithm that solves the modular equation $ax \equiv b \ (mod\, n)$ given the input (a, n, b):

  - $(d, x', y') \leftarrow Extended - Euclid(a, n)$

- if $d|b$ then
  - $x_0 \leftarrow x' \frac{b}{d} \ (mod\ n)$
  - for $i = 1$ to $d - 1$
    - $x_i \leftarrow (x_0 + i\frac{n}{d}) \ (mod\ n)$
  - return $\{x_0, \ldots, x_{d-1}\}$
- else return $\emptyset$

2 Question 2:

$gcd(e, (p-1)(q-1)) = 1$, and therefore by question 1 there is a single solution to the modular equation $ex \equiv 1 \ (mod\ (p-1)(q-1))$. The solution to this equation is the multiplicative inverse of e modulo $(p-1)(q-1)$. Thus, to find d given e, p, q we just have to run the above algorithm with input $(e, (p-1)(q-1), 1)$.