Mathematics 3159B **Bradley Assaly-Nesrallah**
Introduction to Cryptography
Assignment 1, Problem 1 Due Date: September 22, 2020

Solution

1. Suppose that $ax \equiv c \pmod{m}$ where a,c,m are fixed integers.
We want to show that $ax \equiv c \pmod{m}$ for some $x \in \mathbb{Z}$ if and only if gcd(a,m) divides c.
So we prove both directions as follows:

Proof. $\rightarrow$ Suppose that $ax \equiv c \pmod{m}$ has a solution for some $x \in \mathbb{Z}$.
We want to show that gcd(a,m) divides c,
So $ax \equiv c \pmod{m} \implies m|(ax-c) \implies ym = ax - c$ for some $y \in \mathbb{Z} \implies$ c = ax - my.
Note that gcd(a,m)|a and gcd(a,m)|m by definition of gcd so there exists $i, j \in \mathbb{Z}$ such that a=gcd(a,m)∗i and m=gcd(a,m)∗j.
So

$$\begin{aligned} c = ax - my = (gcd(a,m) * i) * x - (gcd(a,m) * j) * y = gcd(a,m) * (i * x) - gcd(a,m) * (j * y) \\ = gcd(a,m)(ix - jy) \end{aligned}$$

So c=gcd(a,m)∗(ix-jy) $\implies$ gcd(a,m)|c as required.
$\leftarrow$ Suppose that gcd(a,m)|c.
We want to show that $ax \equiv c \pmod{m}$ for some $x \in \mathbb{Z}$,
By the EEA gcd(a,m)= ax' + my' for some $x', y' \in \mathbb{Z}$,
Thus (ax' + my')|c $\implies$ k(ax' + my')=c for some $k \in \mathbb{Z}$

$$\begin{aligned} c = k(ax' + my') = kax' + kmy' = akx' + mky' = a(kx') + m(ky') \\ \implies m(ky') = a(kx') - c \implies a(x'k) \equiv c \pmod{m} \end{aligned}$$

Thus $ax \equiv c \pmod{m}$ with x=$(x'k) \in \mathbb{Z}$ as required.
Thus $ax \equiv c \pmod{m} \iff$ gcd(a,m)|c so we are done.

□

2. We now want to show that if there is a solution to the congrence then there are exactly gcd(a, m) distinct solutions in $\mathbb{Z}$/m.

Proof. Suppose that $ax \equiv c \pmod{m}$ has a solution for some $x \in \mathbb{Z}$.
We want to show there are exactly gcd(a,m)=d solutions in $\mathbb{Z}$/m.
By the result in part 1 since the congruence has a solution we know that gcd(a,m)|c, so c=gcd(a,m)∗ for some $k \in \mathbb{Z}$

From the theorem 1.11 if one solution has the form (x',y') for $x', y' \in \mathbb{Z}$ then every solution has the form :

$$x = x' + mk/d \text{ and } y = y' - ak/d \text{ for some k} \in \mathbb{Z}$$

Observe that the solutions must have k=0,+-1,+-2,...
We claim the solutions are of the form x',x'+m/d,x'+2m/d,...,x'+(d-1)m/d, which are all clearly incongruent in $\mathbb{Z}$/m since the difference between them is all less than m, as ((d-1)/d)<1.
So there must be at least d solutions, now we show there are at most d solutions.
Suppose there was a d+1th solution which is not one of the above d solutions given by x=x'+lm/d $l \in \mathbb{Z}$.
Now by Euclid's division lemma l=qd+r with 0≤r<d and x=x'+(ld+r)m/d≡x'+rm/d, but 0≤r<d so it must be one of the d solutions.
Thus there are exactly gcd(a,m)=d solutions in $\mathbb{Z}$/m so we are done.

□