Harry Langford hjd2

Question 4

a) Proof by ~~strong~~ induction

RTP ~~$x^k \equiv y^k \pmod m$~~

$$x \equiv y \pmod m \Rightarrow x^k \equiv y^k \pmod m$$

for $k = 1$

$x \equiv y \pmod m$

this is true by assumption.

Assume that $x^n \equiv y^n \pmod m$

$x^n \equiv y^n \pmod m \Rightarrow$

① $\exists j \in \mathbb{Z} : x^n = y^n + jm \Rightarrow$

since $x \equiv y \pmod m$ by assumption

② $\exists i \in \mathbb{Z} : x = y + im$

Combining ① & ② gives

$\exists i, j \in \mathbb{Z} : x \times x^n = (y + im) \times (y^n + jm) \Rightarrow$

$\exists i, j \in \mathbb{Z} : x^{n+1} = y^{n+1} + m(jy) + m(iy^n)$

$\exists i, j \in \mathbb{Z} : x^{n+1} \equiv y^{n+1} \pmod m$

Since the statement is true for $k = 1$, and the truth of the statement for $k = 1 \wedge k = n \Rightarrow$ the truth for $k = n + 1$, ~~by induction~~ by induction

$x \equiv y \pmod m \Rightarrow$

$\forall k \in \mathbb{Z} : x^k \equiv y^k \pmod m$

Scanned with CamScanner

Include the case $k=0$

$\forall x \in \mathbb{Z}: x^0 = 1$

$\forall y \in \mathbb{Z}: y^0 = 1$

So $\forall x, y, m \in \mathbb{Z}: x^0 \equiv y^0 \pmod{m}$

So $\forall x, y, m \in \mathbb{Z}: (x \equiv y \pmod{m} \Rightarrow \forall k \in \mathbb{N} \; x^k \equiv y^k \pmod{m})$.

b)i) Alice exponentiates by g by a and mods by p
She then sends and records a and works
out K_1 the inverse of a (mod p-1) : ~~a=1+~~
$K_1 a = 1 \pmod{p-1}$
She sends g^a to bob. ~~who~~
who exponentiates by b.
He works out K_2: $K_2 b \equiv 1 \pmod{p-1}$.
Sends it back to alice.
She exponentiates by K_1. Sends g^b to bob.
bob exponentiates by K_2. This gives him g.

ii) Alice starts with g.

Sends $g^a \pmod{p}$
records K_1: $K_1 a \equiv 1 \pmod{p-1}$

Bob exponentiates $g^a \pmod{p}$ by b.
Sends g^{ab}.
records K_2: $K_2 b \equiv 1 \pmod{p-1}$

Alice exponentiates by K_1.

$\exists i \in \mathbb{Z}$: $g^{abK_1} \equiv g^{b(1+i(p-1))} \equiv g^b \times g^{ib(p-1)} \equiv g^b \pmod{p}$
She then sends this to bob.

Bob receives $g^b \pmod{p}$
Exponentiates by K_2

$\exists j \in \mathbb{Z}$: $g^{K_2 b} \equiv g^{1+j(p-1)} \equiv g^1 \pmod{p}$
Bob now has the original message.

iii) Using Euclids Extended algorithm

$K_2 = 4$.

$39^2 \equiv 21 \pmod{79}$

$21^2 \equiv 46 \pmod{79}$

~~So~~ ~~4~~ $46 \times 39^{20} \equiv 1 \pmod{79}$

$46 : 1, 0 \quad 39 : 0, 1$

$7 : 1, -1 \quad 39 : 0, 1$

$7 : 1, -1 \quad 4 : -5, 6$

$3 : 6, -7 \quad 4 : -5, 6$

$1 : -11, 13$

So $39^{20} \equiv -11 \pmod{79}$

$39^{20} \equiv 68 \pmod{79}$

So Alice sends 68.

iv)