PROOFS: HOMEWORK 3

ANDREW TSENG: ART2589

Problem 2.3

Part A Because of FLT and remark 2.3, we can say that:

$$(\exists k_1, k_2 \in Z)(a + k_1(p-1) = b + k_2(p-1) \mod p-1)$$

Since a and b are known integer solutions that solve for the SAME h in the DLP solution, this means that they are in the same congruence class of p. This implies that

$$a \equiv b \mod (p-1)$$

This also shows that the two equations of $a + k(p-1)$ and $b + k(p-1)$ map to the same power in the group $\frac{Z}{(p-1)Z}$, since they solve for the same h. The field F_p^*

Part B Let x, y be integers that solve the following DLP

$$g^x = a \mod p$$

$$g^y = b \mod p$$

By modular arithmetic this means that

$$g^{x+y} = ab \mod p$$

Thus it is obvious that

$$\log_g(a) + \log_g(b) = \log_g(ab)$$
$$x + y = x + y$$

Part C We know that $g^x = h \mod p$ implies that $\log_g(h) = x$.
By mulitplying both sides with an integer n

$$g^{nx} = h^n \mod p$$

This implies the same expression from above

$$\log_g(h^n) = nx = n \log_g(h)$$

Problem 2.24

Part A
$(b + kp)^2 = b^2 + 2kbp + (kp)^2$ We know that $b^2 = gp + a$ so:

$$(b + kp)^2 = gp + a + 2kbp = a + p(g + 2kb) \mod p^2$$

So we are to find a k such that $g + kb \mod p = 0$.

Part B
$p = 1291$, $b = 537$, $a = 476$, $g = 223$, then we find a k such that $g + kb \mod p = 0$.
Using a computer program, $k = 239$ is a solution.

Part C

Part D

Part E

Problem 2.27