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.

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
Given: $(b + kp)^2 = b^2 + 2kbp + (kp)^2$
We know that $b^2 = gp + a$, because b is a sqr root modulo of $a \mod p$:

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

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 with the formula mentioned, $k = 239$ is a solution.

Part C
From the given, we can assume that $b^2 = gp^n + a$ and so $(b + jp^n)^2 = gp^{n+1} + a$.
We find that:

$$gp^n + a + 2bjp^n + p^{2n} = a + gp^{n+1}$$
$$a + p^n(g + 2bj + p^n) = a + gp^{n+1}$$

This implies that if $g + 2bj + p^n \equiv 0 \mod p$ then $b + jp^n$ is a square root modulo of $a \mod p^{n+1}$. We want a j that satisfies that condition.

Part D

Since we know from part a that if $b^2 \equiv a \mod p$ then there is a square root modulo for $a \mod p^2$.

Using induction our base case would be part A. Now we know that the predicate is true for n = 1, then we are to prove that for ever b that is a square root modulo of $a \mod p^n$, then there is a square root modulo for $a \mod p^{n+1}$.

Thus with strong induction, if there exists a square root modulo for $a \mod p$, then there exists a square root modulo for $a \mod p^2, a \mod p^3, a \mod p^4, \ldots, a \mod p^n$.

Part E

Given that, $p = 13, a = 3, b = 9, g = 6$.
$6 + 2(9)j + 169 \equiv 0 \mod p$.
Solution(s): $j = 4, 17$.

Problem 2.27

Pohlig-Hellman solves the solution of x where $g^{x_1 q_1} = h^{q_1}$ and $g^{x_2 q_2} = h^{q_2}$. We could then use CRT to find the solution x such that $x \equiv x_1 \mod q_1$ and $x \equiv x_2 \mod q_2$.

Because q_1, q_2 are prime, we know that $\gcd(q_1, q_2) = 1$ so there exists a a, b such that $aq_1 + bq_2 = 1$. So we can say that: $g^{x(aq_1+bq_2)} = (g^x)^{aq_1}(g^x)^{bq_2} = h^{aq_1}h^{bq_2} = h$.