Homework 3

Due Thursday, September 24

Written Part

5. Let's prove some properties of the discrete logarithm.

   (a) Let g be a primitive root of $\mathbb{F}_p^*$. Fix $a, b \in \mathbb{Z}$ and suppose that $g^a \equiv g^b \mod p$. Show that $a \equiv b \mod (p-1)$.

   Proof. We recall that we showed in class that if $g \in \mathbb{F}_p^*$ has order d, and $g^k \equiv 1 \mod p$, then $d|k$. Since g is a primitive root, its order is $p-1$. Since $g^a \equiv g^b$ we know that $g^{b-a} \equiv 1 \mod p$, so that by what we just said, $p-1$ divides $b-a$, completing the proof. $\square$

   (b) Use part (a) to prove that the discrete log map $\log_g : \mathbb{F}_p^* \longrightarrow \mathbb{Z}/(p-1)\mathbb{Z}$ is well defined.

   Proof. Suppose that a and b both solve $x = \log_g h$. This means $g^a \equiv h \equiv g^b \mod p$ so that by part (a) $a \equiv b \mod p-1$ so that they define the same element of the target. $\square$

   (c) Show that the map $\log_g$ from part (b) is *bijective*. (Hint, can you construct an explicit inverse?).

   Proof. We build an expoential map $g^x : \mathbb{Z}/(p-1)\mathbb{Z} \to \mathbb{F}_p^*$. It is defined in the obvious way, for $a = \{1, 2, ..., p-1\}$ we let,

   $$g^a = \underbrace{g \cdot g \cdots g}_{a \text{ times}}$$

   Then one checks that $\log_g g^a = a$ and $g^{\log_g a} = a$ by definition. $\square$

   (d) Show that $\log_g(ab) = log_g(a) + \log_g(b)$ for all $a, b \in \mathbb{F}_p^*$. (For those of you have seen group theory, this means $\log_g$ is a homomorphism, and in light of (c) an *isomorphism*!)

   Proof. Let $x = \log_g(a)$ and $y = \log_g(b)$. This means $g^x = a$ and $g^y = b$. Therefore $ab = g^x g^y = g^{x+y}$ so that $x + y = \log_g(ab)$. $\square$

6. Let p be an odd prime and g a primitive root of $\mathbb{F}_p^*$. Prove that $a \in \mathbb{F}_p^*$ has a square root if and only if $\log_g(a)$ is even.

   Proof. This is essentially just a rephrasing of problem 8 on homework 2. We showed that if g is a primitive root and $a = g^k$, then a has a square root if and only if k is even. But k is precisely $\log_g a$. $\square$

7. In Homework 2 we studied square roots mod p. Let's use this to study square roots modulo p^e for some positive exponent e. Let p be a prime not equal to 2, and let b be an integer not divisible by p. Suppose further that b has a square root modulo p, i.e., the congruence:

$$x^2 \equiv b \mod p,$$

has a solution.

(a) Show that for every exponent $e \geq 1$, b has a square root module p^e. That is, the congruence

$$x^2 \equiv b \mod p^e$$

has a solution. (**Hint:** Use induction on e, finding a solution modulo p^{e+1} by modifying the solution modulo p^e.)

Proof. The following lemma will be very helpful:

Lemma 1. *Let $a, b \in \mathbb{Z}$. Then $(a+b)^p = a^p + b^p + pab(stuff)$.*

Proof. The binomial theorem says:

$$(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i}$$

Pulling out the terms for $i = 0$ and $i = p$ this becomes:

$$(a+b)^p = a^p + b^p = \sum_{i=1}^{p-1} \binom{p}{i} a^i b^{p-i}$$

Since a and b divide each term in the sum, it only remains to show $\binom{p}{i}$ is divisible by p for each $i = 1, \cdots, p-1$. Recall that,

$$\binom{p}{i} = \frac{p!}{i!(p-i)!},$$

which has a factor of p in the numerator. But all the factors in the denominator are smaller than p, so the factor of p in the numerator cannot be cancelled out. □

With this lemma in hand we prove the result. We will induct on e. For $e = 1$ we are assuming b has a square root. For the general case we may let β be a square root of b modulo p^e. This means that there is some integer k such that:

$$\beta^2 = b + kp^e.$$

One can raise both sides of this equation to the pth power and apply the Lemma:

$$\beta^{2p} = b^p + k^p p^{pe} + (b)(kp^e)(p)(\text{stuff}).$$

In particular:

$$\beta^{2p} \equiv b^p \mod p^{e+1}.$$

As b is not divisible by p, $\gcd(b, p^e) = 1$ so that we can divide the congruence above by b. In fact, we divide by b^{p-1} so we can solve for b.

$$b^{1-p}\beta^{2p} \equiv b \mod p^{e+1}.$$

Lastly, we notice that $1-p$ is even, so that the right hand side of the congruence becomes:

$$b^{1-p}\beta^{2p} = \left(b^{\frac{1-p}{2}}\beta^p\right)^2,$$

so that we see $b^{\frac{1-p}{2}}\beta^p$ is a square root of b modulo p^{e+1}. □

We present a second proof for the inductive step which, although perhaps not quite as neat, may be easier to find. The goal is see that if $\beta^2 \equiv b \mod p^e$, then and x were a square root mod p^{e+1}, then x would also be a square root mod p^e, so perhaps it is reasonable to expect that $x \equiv \beta \mod p^e$. This would mean that $x = \beta + kp^e$. Then

$$x^2 = \beta^2 + 2kp^e + p^{2e} \equiv \beta^2 + 2p^e \equiv \beta^2 + 2kp^e \mod p^{e+1},$$

where the last step holds because $2e \geq e + 1$. Therefore it remains to choose a k such that

$$\beta^2 + 2kp^e \equiv b \mod p^{e+1}.$$

By assumption β is a square root of b mod p. We know that $\beta^2 = b + lp^e$ (for some *fixed* l), so we must solve:

$$b + lp^e + 2kp^e \equiv b \mod p^{e+1},$$

for k. This reduces to:

$$(l + 2k)p^e \equiv p^{e+1},$$

so we must find some k such that $p|(l + 2k)$. We can always do this because p is an odd prime (if l is odd then $l + 2k$ spans the odd numbers as we vary k, so just choose a k such that $l + 2k = p$, else $l + 2k$ spans the evens so we may choose a k such that $l + 2k = 2p$). In particular, we have found a value of k so that if $x = \beta + kp^e$ then x is a square root of $b \mod p^{e+1}$.

(b) Let $x = \alpha$ be a square root of b modulo p. Prove that in part (a) we can find a square root root β of $b \mod p^e$ such that $\alpha \equiv \beta \mod p$.

Proof. Supose $\beta^2 \equiv b \mod p^e$. Then in particular we know $\beta^2 \equiv b \mod p$. By HW2 Problem 8(a) we know $\beta \equiv \pm\alpha \mod p$. If $\beta \equiv \alpha \mod p$ then we are done, otherwise if we replace β with $-\beta$ we see that

$$(-\beta)^2 = \beta^2 \equiv b \mod p^e,$$

so that $(-\beta)$ is a square root of $b \mod p^e$ which is congruent to $\alpha \mod p$ as desired. □

(c) Suppose β, β' are two square roots of b mod p^e, and further that they are both equivalent to $\alpha \mod p$ as in part (b). Show that $\beta \equiv \beta' \mod p^e$.

Proof. Since $\beta \equiv \beta' \equiv \alpha \mod p$, then we know that $\beta + \beta' \equiv 2\alpha \mod p$. Since p is odd, $2\alpha \not\equiv 0 \mod p$, so that p does not divide $\beta + \beta'$.
By assumption, p^e divides $\beta^2 - \beta'^2 = (\beta - \beta')(\beta + \beta')$. But in the first paragraph we showed that $\gcd(p^e, \beta + \beta') = 1$, so that in fact $p^e|(\beta - \beta')$ completing the proof. □

(d) Conclude that the congruence $x^2 \equiv b \mod p^e$ has either 2 solutions or 0 solutions. (Use HW2 Probem 8).

Proof. Suppose there aren't 0 solutions. We let β is a solution, and let α be reduction of $\beta \mod p$. Then $-\beta$ is another solution. If γ is a third solution the $\gamma \equiv \pm\beta \mod p$ by HW2 Problem 8(a), so that by part (c) above we have that $\gamma \equiv \pm\beta$. So there are exactly 2 solutions □

Recall in class we proved that the Discrete Logarithm Problem (DLP) is harder than the Diffie-Hellman Problem (DHP). Explicitely, we showed that if you have a solution to the DLP you can use this to solve the DHP. We finish this assignment with a proof of this sort, following [HPS Exercise 2.7]. We first must introduce the following problem:

Definition 1. *The decision Diffie-Hellman Problem (dDHP) is a s follows. Suppose that you are given 3 number A, B, and C, and suppose A and B are equal to*

$$A \equiv g^a \mod p \quad \textit{and} \quad B \equiv g^b \mod p,$$

for some (unknown) a and b. Determine whether $C \equiv g^{ab} \mod p$.

This is the first of several of *decision* variants of problems we will see. Notice the DHP asks you to compute g^{ab} where as the dDHP just asks you to check if a given set of data is the solution.

8. (a) Show that the DHP is harder than the dDHP. That is, show a solution to the DHP gives a solution to the dDHP.

Proof. Suppose you had a DHP oracle which could solve the DHP for you. Next suppose you are given A, B, and C as in the dDHP. To solve the dDHP you consult your DHP oracle, who tells you $g^{ab} \mod p$. You may then check if this solution is congruent to C. □

(b) Do you think the dDHP is hard or easy? Why?
This is really an open ended question. Part (a) makes it seem like it is much easier than the DHP, since a solution to the DHP immediately solves the dDHP. The converse seems unlikely, having a dDHP oracle doesn's seem to give a better way to solve the DHP other than guessing values of C and using the dDHP oracle to check if they were correct.

There is a way in that the dDHP is in fact more tractable than the DHP. First notice that if we take $(g^x)^{(p-1)/2}$ this is 1 if x is even (by Fermat's little theorem) and -1 if x is odd. Therefore we can compute quickly whether a, b, ab are even or odd, and get an easy negative answer if the necessary parity doesn't hold. If $p \equiv 3 \mod 4$ we have seen in class how to compute square roots, so this could be the basis of an inductive algorithm to solve the dDHP.