Applied Number Theory: Homework 3

Joshua Dong

September 26, 2016

2.3

a)

g is a primitive root of $\mathbb{F}_p$. Then g is a generator of the group. Then the order of g is p, and $g^p = 1$. Then g^n for $n \in \{0, 1, 2, ..., p-1\}$, g^n is distinct for different n, and $g^n = g^{n+(p-1)}$. This effectively defines p unique, disjoint equivalence classes for the elements in $\{g^n | n \in \mathbb{Z}\}$.

If $x = a$, a solution to $g^x = h$, then where a is in the equivalence class A (since equivialence classes are disjoint and cover the space). If $x = b$, then b must also be in the class A, by definition of our equivialence class. Since the elements of A may be expressed as $A = \{a + k(p-1) | k \in \mathbb{Z}\}$. Then $p - 1 | a - b$.

b)

Let $a, b, c \in \mathbb{F}_p^*$ such that $g^a = h_1 h_2$, $g^b = h_1$, $g^c = h_2$ for any given $h_1, h_2 \in \mathbb{F}_p^*$.

Then $g^b g^c = h_1 h_2$. Then $g^{b+c} = h_1 h_2$. Then $g^{b+c} = g^a$, $a = b + c$ as could be clearly proven by a uniqueness argument for the equivalence classes in $\mathbb{F}_p^*$.

$a = \log_g h_1 h_2$, $b = \log_g h_1$, $c = \log_g h_2$ by definition of logarithm. Then $\log_g h_1 h_2 = \log_g h_1 + \log_g h_2$, which is what we sought to show.

c)

Let $a, b \in \mathbb{F}_p^*$ such that $g^a = h^n$, $g^b = h$ for any given $h \in \mathbb{F}_p^*, n \in \mathbb{Z}$.

Then $g^{nb} = (g^b)^n = h^n$. Then $a = nb$.

$a = \log_g h^n$, $b = \log_g h$ by definition of logarithm. Then $\log_g h^n = n \log_g h$, which is what we sought to show.

2.24

a)

It is given that $b^2 - a = np$ for some $n \in \mathbb{Z}$, and p is odd and does not divide b. Since p is odd and does not divide b, we can find a $k \in \mathbb{Z}$ such that $k \equiv (2b)^{-1}(-n) \mod p$ for some given $n \in \mathbb{Z}$.
Then there exists a $k \in \mathbb{Z}$ such that $(n + 2bk) \equiv 0 \mod p$ for some given $n \in \mathbb{Z}$.
Then for these k, n, there exists a $m \in \mathbb{Z}$ such that $p(n + 2bk) = p(mp)$.
Then $0 \equiv np + 2bk \equiv (b^2 - a) + 2bkp + (kp)^2 \equiv p(b + kp)^2 - a \mod p^2$.
Then $a \equiv (b + kp)^2 \mod p^2$, which is what we sought to show.

b)

309086

c)

$b^2 - a \equiv 0 \mod p^n$.
Since $2b$ is even and p is odd and does not divide b, $2b$ is invertable.
Then there exists $j \in \mathbb{Z}$ such that $j \equiv (-k)(2b)^{-1} \mod p$ where $k(p^n) = b^2 - a$.
Then there exists $j \in \mathbb{Z}$ such that $2bj + k \equiv 0 \mod p$, $(2bj + k)p^n \equiv 0 \mod p^{n+1}$.
Then there exists $j \in \mathbb{Z}$ such that $(b^2 - a) + (jp^n)^2 + (2b)jp^n \equiv 0 \mod p^{n+1}$.
Then there exists $j \in \mathbb{Z}$ such that $b^2 + (jp^n)^2 + (2b)jp^n \equiv a \mod p^{n+1}$.
Then there exists $j \in \mathbb{Z}$ such that $(b + jp^n)^2 \equiv a \mod p^{n+1}$, which is what we sought to show.

d)

We can apply the principle of mathematical induction. Let $P(n) :=$ If p is an odd prime and if a has a square root modulo p^n, then a has a square root modulo $p^n + 1$. We already have shown $P(1)$ and $P(n) \to P(n+1)$. Then $P(n)$ is true for all integers n.

One of the core assumptions was that p is odd, since this guarantees invertability for $2b$. Thus, $P(n)$ does not hold if the prime used is 2.

e)

1075 as well as 1122 are the square roots of 3 modulo 13^3, since 4 is also a square root of 3 modulo 13.

2.27

Let G be a group with order $\varphi(p) = q_1q_2$, where p is a prime number. Let $g \in G$, en element of order N. N can be factored into a product of primes as $N = q_1 \cdot q_2$.

Then we can break the problem of the discrete logorithm of $h = g^x \mod p$ (given some arbitrary h) into the smaller problems of discrete logarithm modulo q_1 and q_2.

By the Chinese Remainder Theorem, x can be retrieved by way of combining the solutions of the modular equations $h = g^{y_1} \mod q_1$ and $h = g^{y_2} \mod q_2$.

Suppose we have:
$x = y_1 + q_1z_1$ for some $z_1 \in \mathbb{Z}$ and $x = y_2 + q_2z_2$ for some $z_2 \in \mathbb{Z}$.

Then $(g^x)^{q_2} = (g^{y_1+q_1z_1})^{q_2}, (g^x)^{q_1} = (g^{y_2+q_2z_2})^{q_1}$,
q_1, q_2 are coprime. Then by Bezout's theorem, there exists c_1, c_2 such that $q_1c_1 + q_2c_2 = 1$.

Since $q_2x \equiv q_2 \log_g(h)(\mod N), q_1x \equiv q_1 \log_g(h)(\mod N)$.
Then $(q_2c_2 + q_1c_1)x \equiv (q_2c_1 + q_1c_2) \log_g(h)(\mod N)$.
Then $x \equiv \log_g(h)(\mod N)$, which is what we sought to show.

Now the discrete logarithm problem has been broken up into two much smaller discrete logarithm problems.