Homework 2

Erik Brakke

September 17, 2015

Collaborators: None .

Answer 1

(a) Thm: If $x \equiv y \pmod{p-1}$ then for any $a, a^x \equiv a^y \pmod{p}$

Proof: $x = (p-1)k_x + r$ and $y = (p-1)k_y + r$ (by the unique fact about division)
Consider, $a^{(p-1)k_x+r} \equiv a^{(p-1)k_y+r} \pmod{p}$ (using substitution)
$a^{(p-1)k_x+r} \bmod p = a^{(p-1)k_y+r} \bmod p$ (fact about congruency)
$(a^{(p-1)})^{k_x} \bmod p * a^r \bmod p = (a^{(p-1)})^{k_x} \bmod p * a^r \bmod p$ (property of exponents and proof from HW1 that the order of 'mod' does not matter)
$1 * a^r \bmod p = 1 * a^r \bmod p$ (by Fermat's little theorm)
$a^r \equiv a^r$
(fact about congruency)
$r = x \bmod p-1 = y \bmod p-1$ (by definition of 'mod' and our premise)
Therefore, if $x \equiv y \pmod{p-1}$ then for any $a, a^x \equiv a^y \pmod{p}$

□

(b) Thm: if g is a generator, then $g^x \equiv 1$ if and only if $(p-1) \mid x$

Proof: Assume $g^x \equiv 1$
$g^{p-1} \equiv 1$ ($g \in Z_p^*$ by def'n of generator, Fermat's Little Theorm)
$x = p-1$ (substitution)
Therefore, $(p-1) \mid x$ (definition of divides)

Now, assume $(p-1) \mid x$
Let $r = x \bmod (p-1)$ (Def'n of 'mod')
$r = 0$ (def'n of divides)
Consider $g^r \pmod{p}$
$g^{x \bmod p-1}$ (substitution)
$g^0 = 1$ (becasue $(p-1) \mid x$)
Therefore $g^x \equiv 1$

□

(c) Thm: if g is a generator, and $g^x \equiv g^y$ then $x \equiv y \pmod{p-1}$

Proof: Let's assume $g^x \equiv g^y$ and $x \not\equiv y \pmod{p-1}$

$x \bmod p-1 \neq y \bmod p-1$ (Fact of congruency)
$r_x \neq r_y$ (definition of mod)
This means that $\exists_{r_x,r_y}\ r_x r_y \in (1,...,p-1), r_x \neq r_y$ and $g^{r_x} \equiv g^{r_y}$
However, g is a generator, which means that each element in $(1,...,p-1)$ maps to a distinct element in $(1,...,p-1)$ (def'n of generator)
Therefore, $g^{r_x} \not\equiv g^{r_y}$ which means $g^x \not\equiv g^y$
This is a contradiction, therefore the statement must be true □

(d) Thm: If g is a generator, and $a = g^x \pmod p$, and x is even, then a has a square root modulo p

Proof: Because x is even, we can rewrite it as $2y$ where y is also a number in {1,...,p-1}
$a = g^{2y} \bmod p$
$a = (g^y \bmod p) * (g^y \bmod p)$ (Splitting exponents with like bases)
Because g is a generator, we know that $g^y \in \{1,...,p-1\}$ and $g^y \not\equiv g^x$ (def'n of generator)
Therefore g^y is the square root of a (Knowledge of square roots)

□

Thm: if a has a square root modulo then x is even

Proof: Let's represent a as a generator g raised to some x mod p. $a = g^x \bmod p$
Let's also assume that x is odd
$g^x \equiv g^y * g^y$ (because we assume that a has a square root)
$g^x \equiv g^{2y}$
This means that $x = 2y$
This is a contradiction, because we assumed x was even
Therefore, if a has a square root, then x must be even. □

(e) Thm: If a is a square, then $a^{\frac{p-1}{2}} \equiv 1$

Proof: Let's assume there is a generator g such that $g^x \equiv a$
We know that x must be even (by the previous part)
$x = 2y$ for some $y \in \{1,...,p-1\}$
$a \equiv g^{2y}$
Now consider $(g^{2y})^{\frac{p-1}{2}}$
$g^{y(p-1)}$ (2's cancel)
Because $(p-1) \mid y(p-1)$ we know that $g^{y(p-1)} \equiv 1$ (proof from (b))
Therefore, $a^{\frac{p-1}{2}} \equiv 1$

□

Thm: If a is non-square, then $a^{\frac{p-1}{2}} \not\equiv 1$

Proof: Let's assume there is a generator g such that $g^x \equiv a$
We know that x must be odd (from proof (d))
Now consider $(g^x)^{\frac{p-1}{2}}$
$g^{\frac{x}{2}(p-1)}$ (using rules of exponents)
$(p-1) \nmid \frac{x}{2}(p-1)$ therefore, $a^{\frac{p-1}{2}} \not\equiv 1$

□

(f) Thm: If $(g^x)^2 \equiv a$ then $(g^{x+(p-1)/2})^2 \equiv a$

Proof: We can rewrite a as g^{2x} (Rules of exponents)
Now let's rewrite the latter expression:
$g^{2(x+(p-1)/2)} \equiv g^{2x} * g^{p-1}$ (Rules of exponents)
This can be rewritten as $g^{2x} * 1$ (by Fermat's Little Theorm)
Therefore, $a \equiv (g^{x+(p-1)/2})^2$

□

Thm: $g^{(p-1)/2} \equiv -1$

Proof: Consider $(g^{(p-1)/2})^2$
$g^{p-1} \equiv 1$ (Rules of exponents and Fermat's Little Therom)
Therefore, we know that $g^{(p-1)/2}$ is the square root of 1
We know that $-g^x \equiv g^{x+(p-1)/2}$ (From the facts stated)
Let's assign $x = (p-1)/2$
$-g^{(p-1)/2} \equiv g^{2(p-1)/2}$ Therefore, $-g^{(p-1)/2} \equiv 1$ (Fermat's Little Theorm)
Therefore, $g^{(p-1)/2} \equiv -1$ (Multiplication)

□

Thm: If b is non-square, then $b^{(p-1)/2} \equiv 1$

Proof: Let $g^z \equiv b$
We know that z is odd (by proof (d))
We can rewrite this as $g * g^x \equiv b$ where x is an even number
Let $a \equiv g^x$ be a square (because x is even) Now, consider $(g * a)^{(p-1)/2}$
$g^{(p-1)/2} * a^{(p-1)/2}$
We know that $a^{(p-1)/2} \equiv 1$ (From part (e)) and $g^{(p-1)/2} \equiv -1$ (from previous part)
Therefore, $-1 \equiv b^{(p-1)/2}$

□

(g) Thm: If $p \equiv 4 \pmod 4$, and a has a square root, then $a^{(p+1)/4}$ is a square root of a

Proof: If $p \equiv 3$ then $(p+1)/4 = 2$ which is an integer
Now, let's consider $(a^{(p+1)/4})^2$
Rewritten $a^{(p+1)/2}$
$a * a^{(p-1)/2}$
Therefore, $(a^{(p+1)/4})^2 \equiv a$ (From part(e) $a^{(p-1)/2} \equiv 1$)
Therefore, $a^{(p+1)/4}$ is a square root of a

□

Answer 2

We know the $\Pr[Win] = f(k)$ if the lottery is played one time
If a player played $p(k)$ times, where p is a polynomial, then $\Pr[Win] = \Pr[Win(1) OR Win(2) OR ... OR Win(k)]$
This can be written as $\Pr[Win] \leq \sum_1^k f(k)$ (Upper bound)
This is also $\Pr[Win] \leq k * f(k)$
And because we know that $f(k)$ is negligble in the size of k, then we can also say $k * f(k)$ is negligible (Definition of negligible)
Therefore, the upper-bound on the probabily of winning is negligible, therefore the chances of winning are still negligible

Answer 3

Thm: If the discrete logarithm problem holds, then given g^{xy} and g^y, it is hard to computer x

Proof: First, let's try to isolate g^x
To do so, we can take the g^y root of both sides
$(g^{xy})^{1/y} = g^x$
Great! However, in order to get x, we solve $\log_g(g^x)$
This means we have to find the discrete log, which we assumed was hard. Therefore, finding x is a hard problem

$\square$

Thm: For any poly-time algorithm A, there exists a negligible function η such that, if you generate a k bit p and its generator g and select a random $x, y \in \mathbb{Z}_p^*$, $\Pr[A(p, g, g^{xy} \bmod p), g^y \bmod p) = x] \leq \eta(k)$

Proof: Let's assume that there does exist a poly-time algorithm A such that $\Pr[A(p, g, g^{xy} \bmod p), g^y \bmod p) = x] > \eta(k)$
Now, let's use algorithm A to solve the discrete log problem
If we give $A(p, g, g^{xy} \bmod p, g^y \bmod p)$, then there is a non-negligible chance that A will output x
And because we have assumed that A is a poly-time algorithm, this means that the discrete log problem can be solved in poly time
However, we assume that the discrete log problem is hard, and in poly-time we cannot get x from $p, g, g^{xy} \bmod p, g^y \bmod p$
We have arrived at a contradiction, therefore such an A does not exist

$\square$

References

None