

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)
 $a^{(p-1)k_x+r} \pmod{p} = a^{(p-1)k_y+r} \pmod{p}$ (fact about congruency)
 $(a^{(p-1)})^{k_x} \pmod{p} * a^r \pmod{p} = (a^{(p-1)})^{k_y} \pmod{p} * a^r \pmod{p}$ (property of exponents and proof from HW1 that the order of 'mod' does not matter)
 $1 * a^r \pmod{p} = 1 * a^r \pmod{p}$ (by Fermat's little theorem)
 $a^r \equiv a^r$
 (fact about congruency)
 $r = x \pmod{p-1} = y \pmod{p-1}$ (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 $g^x \equiv 1$
 $g^{p-1} \equiv 1$ ($g \in \mathbb{Z}_p^*$ by def'n of generator, Fermat's Little Theorem)
 $x = p-1$ (substitution)
 Therefore, $(p-1) \mid x$ (definition of divides)

Now, assume $(p-1) \mid x$
 Let $r = x \pmod{p-1}$ (Def'n of 'mod')
 $r = 0$ (def'n of divides)
 Consider $g^r \pmod{p}$
 $g^{x \pmod{p-1}} \pmod{p}$ (substitution)
 $g^0 = 1$ (because $(p-1) \mid x$)
 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 $\exists_{r_x, r_y} r_x r_y \in (1, \dots, p-1), r_x \neq r_y$ and $g^{r_x} \equiv g^{r_y}$

However, g is a generator, which means that each element in $(1, \dots, p-1)$ maps to a distinct element in $(1, \dots, p-1)$ (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 \square

(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 $\{1, \dots, p-1\}$

$a = g^{2y} \pmod{p}$

$a = (g^y \pmod{p}) * (g^y \pmod{p})$ (Splitting exponents with like bases)

Because g is a generator, we know that $g^y \in \{1, \dots, p-1\}$ and $g^y \neq g^x$ (def'n of generator)

Therefore g^y is the square root of a (Knowledge of square roots) \square

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

Proof: Let's represent a as a generator g raised to some $x \bmod p$. $a = g^x \pmod{p}$

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. \square

(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 $y \in \{1, \dots, p-1\}$

$a \equiv g^{2y}$

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, $a^{\frac{p-1}{2}} \equiv 1$ \square

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, $a^{\frac{p-1}{2}} \not\equiv 1$ \square

(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:

$$g^{2(x+(p-1)/2)} \equiv g^{2x} * g^{p-1} \text{ (Rules of exponents)}$$

This can be rewritten as $g^{2x} * 1$ (by Fermat's Little Theorem)

$$\text{Therefore, } a \equiv (g^{x+(p-1)/2})^2$$

□

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

Proof: Consider $(g^{(p-1)/2})^2$

$$g^{p-1} \equiv 1 \text{ (Rules of exponents and Fermat's Little Theorem)}$$

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 $x = (p-1)/2$

$$-g^{(p-1)/2} \equiv g^{2(p-1)/2} \text{ Therefore, } -g^{(p-1)/2} \equiv 1 \text{ (Fermat's Little Theorem)}$$

$$\text{Therefore, } g^{(p-1)/2} \equiv -1 \text{ (Multiplication)}$$

□

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)

$$\text{Therefore, } -1 \equiv b^{(p-1)/2}$$

□

(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 $\Pr[\text{Win}] = f(k)$ if the lottery is played one time

If a player played $p(k)$ times, where p is a polynomial, then $\Pr[\text{Win}] = \Pr[\text{Win}(1) \text{OR} \text{Win}(2) \text{OR} \dots \text{OR} \text{Win}(k)]$

This can be written as $\Pr[\text{Win}] \leq \sum_1^k f(k)$ (Upper bound)

This is also $\Pr[\text{Win}] \leq k * f(k)$

And because we know that $f(k)$ is negligible in the size of k , then we can also say $k * f(k)$ is negligible (Definition of negligible)

Therefore, the upper-bound on the probability 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 compute x

Proof: $g^{xy} = (g^y)^x$

We can find x by $\log_{g^y}(g^{xy})$

This is the discrete logarithm problem. So it is hard to compute x

□

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 $\Pr[A(p, g, g^{xy} \bmod p), g^y \bmod p) = x] > \eta(k)$

Let's have another algorithm $D(p, g^{xy}, g^y) = x$ that uses A to solve the discrete log problem

If we generate a random $g \in \{1, 2, \dots, p-1\}$, then we can pass p, g^{xy}, g^y, g along to A to solve for x

$\Pr[A(p, g, g^{xy}, g^y) = x | g \text{ was correctly guessed}] = f(x)$ Where f is some non-negligible function

$\Pr[A(p, g, g^{xy}, g^y) = x | g \text{ was guessed incorrectly}] = \frac{1}{p} * \frac{p-1}{p}$

Therefore, the event that x is guessed correctly is $f(x) + \frac{1}{p} * \frac{p-1}{p}$

This is a greater than negligible chance that x is correct, meaning that D can solve for x with greater than negligible change

This is a contradiction because D is hard to do in poly time. Therefore, A is correct with less than negligible change

□

References

None