1	2	3	4	5	6	7	8

Lisa Maszkiewicz

4/16/20 Problem Set #4

3. a) The final equation is: $x_1 = y_1^{c_1}(y_2^{c_2})^{-1} \bmod n$, to show it will equal the original plaintext x, we will keep substituting to get x on the right side. $c_1 = b_1^{-1} \bmod b_2$, $c_2 = (c_1 b_1 - 1)\frac{1}{b_2}$

$$x_1 = y_1^{\wedge b_1^{-1} \bmod b_2}\left(y_2^{(c_1 b_1 - 1)1/b_2}\right)^{-1} \bmod n$$

next substitute $y_1 = x^{b_1} \bmod n$ & $y_2 = x^{b_2} \bmod n$

$$x_1 = x^{\cancel{b_1 b_1^{-1}} \bmod b_2}\left(x^{\cancel{b_2}(c_1 b_1 - 1)\cancel{1/b_2}}\right)^{-1} \cancel{\bmod n}$$

sub c_1

$$= x^{\cancel{1 \bmod b_2}^{1}}\left(x^{b_1^{-1} \bmod b_2 \cancel{b_1} - 1}\right)^{-1} \bmod n$$

$$= x^1\left(x^{\cancel{1 \bmod b_2 - 1}^{0}}\right)^{-1} \bmod n$$

$$= x\,(\cancel{x^0})^{\cancel{-1}\,1} \bmod n$$

✓ $x_1 = x$ ■ So Alice will be able to get the plaintext.

7. Suppose: p is prime, $x^2 \equiv 1 \bmod p$
Prove: $x \equiv 1 \bmod p$ or $x \equiv -1 \bmod p$

Proof: By Thm 3.2 i) $a \equiv b \pmod m \Leftrightarrow (a-b)$ ~~[illegible]~~ is a multiple of m
$\Rightarrow (x^2-1)$ is a multiple of p
$\Rightarrow p \mid (x^2-1) = p \mid (x+1)(x-1)$

Then by Thm 1.14) If $d \mid ab$ and $a \perp d$, then $d \mid b$
$p \mid (x+1)(x-1)$, $p \perp (x+1)$ or $p \perp (x-1)$ bc p is prime, it is relatively prime to at least one of them. Therefore, for example say $p \perp (x+1)$, then $p \mid (x-1)$. Or, say $p \perp (x-1)$, then $p \mid (x+1)$. ■

Thm 2.2 expresses this better. "If p is prime & $p \mid ab$, then $p \mid a$ or $p \mid b$." ∴ Since p is prime and

3.2 i) again $p \mid (x+1)(x-1)$, then $\boxed{p \mid (x+1) \Rightarrow x \equiv -1 \bmod p}$ or $\boxed{p \mid (x-1) \Rightarrow x \equiv 1 \bmod p.}$ ■

Lisa Maszkiewicz

Problem Set #4 cont. 4/16/20

4. Given definitions of parity & half, prove that if half(x^e mod n) = 1, then parity($(2x)^e$ mod n) = 1

Proof: if half(x^e mod n) = 1, then $\frac{n}{2} < x \bmod n < n$ by def.

$2x\left(\frac{n}{2} < x < n\right) \Rightarrow n < 2x < 2n \Rightarrow 2x - n$ (= 2x mod n)

$\Rightarrow 2x \bmod n = 2x - n$. 2x is obviously even by defintion of even numbers. Since we know n is odd by definition of RSA, we know $2x-n$ is odd because even # - odd # = odd #.

$\therefore 2x \bmod n = \text{odd} \Rightarrow \text{parity}((2x)^e \bmod n) = 1$. ■

6. Prove that if $a^r \equiv 1 \bmod p$, p is prime, and $d = \gcd(r, p-1)$, then $a^d \equiv 1 \bmod p$

Proof: $\gcd(r,p-1) \mid r$, $\gcd(r,p-1) \mid (p-1)$ then by Prop 1.4 iii $\Rightarrow \gcd(r,p-1) \mid rx + (p-1)y$ (for ~~any~~ ~~some~~ some $x, y \in \mathbb{Z}$)

substitute into $a^d \equiv 1 \bmod p$, $d = \gcd = rx + (p-1)y$

$a^{\wedge rx+(p-1)y} \equiv 1 \bmod p \Rightarrow (a^r)^x \cdot (a^{p-1})^y \equiv 1 \bmod p$

By Fermat's Little Theorem: If p is prime & $a \perp p \Rightarrow a^{p-1} \equiv 1 \bmod p$. We are given that p is prime, we can also easily pick a case where $a \perp p$.

$\therefore (a^r)^x \bmod p \cdot (a^{p-1} \bmod p \equiv 1 \bmod p)^y \equiv 1 \bmod p$

$\Rightarrow (a^r \bmod p)^x \cdot [(1 \bmod p)^y = 1] \equiv 1 \bmod p$

↳ we know $a^r \bmod p = 1 \bmod p$ from the given

$\Rightarrow (1 \bmod p)^x = 1 \cdot 1 \equiv 1 \bmod p$ ✓

$\therefore$ if $a^r \equiv 1 \bmod p$ (& other conditions), then $a^d \equiv 1 \bmod p$

Lisa Maszkiewicz

Problem Set #4 cont.

8. Prove that if $x \equiv y \pmod{\phi(m)}$, then ~~$\forall a \in \mathbb{Z}$~~ ← My pen ran out, guess it's ready to be done with this homework too.

$\forall a \in \mathbb{Z}_m^*$, $a^x \equiv a^y \pmod m$

Proof: If $x \equiv y \pmod{\phi(m)}$, $\pmod{\phi(m)} \mid (x-y)$

$\Rightarrow$ $x = y + k\phi(m)$ for some $k \in \mathbb{Z}$

Plug x into $a^x \equiv a^y \bmod m$

$\Rightarrow a^{y+k\phi(m)} \equiv a^y \bmod m \Rightarrow a^y (a^{\phi(m)})^k \equiv a^y \bmod m$

By Euler's (Thm 4.4) $a^{\phi(m)} \equiv 1 \bmod m$ (We know $a \perp m$ because $a \in \mathbb{Z}_m^*$, by def. of $\mathbb{Z}_m^*$

$\mathbb{Z}_m^* = \{a : 1 \le a \le m \ \& \ a \perp m\}$.

$\Rightarrow a^y (\cancel{1 \bmod m})^{\cancel{k}\,1} \equiv a^y \bmod m$

$\Rightarrow a^y \equiv a^y \bmod m$ ✓ ∎