Math 300.2 Quiz 4 Spring 2016

Name: Solution

1) (20 points) Find all the solutions to the congruence $x^2 \equiv 1^2 \pmod 8$. How may congruence classes in $\mathbb{Z}_8$ solve this congruence?

x	0	1	2	3	4	5	6	7
x^2	0	1	4	1	0	1	4	1

Four congruence classes solve the equation $[x]^2 = [1]$ in $\mathbb{Z}_8$, $\{[1], [3], [5], [7]\}$.

2 (80 points) Prove that the following statement holds for every positive prime integer p:

$$x^2 \equiv y^2 \pmod p \iff ([x \equiv y \pmod p] \text{ OR } [x \equiv -y \pmod p]).$$

We will use:

Prop: Let p be a prime. Then $p \mid ab$ if and only if $p \mid a$ or $p \mid b$, for every $a, b \in \mathbb{Z}$.

$x^2 \equiv y^2 \pmod p \iff p \mid (x^2 - y^2) \iff p \mid (x-y)(x+y) \iff$

$\iff$ ($p \mid (x-y)$ OR $p \mid (x+y)$) $\iff$ $[x \equiv y \pmod p]$ OR $[x \equiv -y \pmod p]$

↑ by the above Proposition

Please use back page for extra space.