

MA 341 - Number Theory
Square Roots of One (mod n)

1) If p is an odd prime

$$x^2 \equiv 1 \pmod{p}$$

has only two solutions, namely $x \equiv \pm 1 \pmod{p}$.

Note: You should be able to show this using $x^2 - 1 = (x + 1)(x - 1)$.

2) If p is an odd prime and $e > 1$ then

$$x^2 \equiv 1 \pmod{p^e}$$

also has only two solutions, namely $x \equiv \pm 1 \pmod{p}$.

Note: You should also be able to show this, however you need to be CAREFUL since when $e > 1$, $p^e \mid ab$ **does not** imply $p^e \mid a$ or $p^e \mid b$ in general. You need to consider the two possible solutions in 1) to show this property holds here.

3) When n is an odd composite number one can show that

$$x^2 \equiv 1 \pmod{n}$$

has more than two solutions. It still has the solutions $\pm 1 \pmod{n}$, called trivial solutions, but it also has other solutions, called non-trivial solutions.

Precisely if n is an odd number and $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ where p_1, \dots, p_r are distinct primes then the equation $x^2 \equiv 1 \pmod{n}$ has exactly 2^r distinct solutions \pmod{n} .

One proves this using the Chinese Remainder Theorem, as we will explain in class. You should understand this proof.

As a special case consider solutions to $x^2 \equiv 1 \pmod{m}$ when $m = p \cdot q$ is the product of two distinct odd primes. The two non-obvious solutions can be found by solving:

$$\begin{array}{ll} 1) & x \equiv 1 \pmod{p} \\ & x \equiv -1 \pmod{q} \\ 2) & x \equiv -1 \pmod{p} \\ & x \equiv 1 \pmod{q} \end{array}$$

Note that the solutions to 1) and 2) will satisfy $x^2 \equiv 1 \pmod{m}$ but will not equal $\pm 1 \pmod{m}$.

The above observations are relevant to modern number theory and its applications to computer science because it gives one way of showing an odd number is composite **without** finding a factor (which is computationally difficult). Specifically, if a number n has a non-trivial square root of one, then it must be composite. We will soon learn another way numbers can be shown to be composite without factoring them.

NOTE: $x^2 \equiv 1 \pmod{2^e}$ can be shown to have 2^{e-1} solutions. In particular the smallest integer n where $x^2 \equiv 1 \pmod{n}$ has more than two solutions is $n = 8$ which can easily be seen to have 4 solutions.

The general formula for the number of solutions to $x^2 \equiv 1 \pmod{m}$ is thus easily seen to be $2^{e-1} \cdot 2^r$ if $n = 2^e p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$. However since even numbers larger than two are obviously composite this is less relevant to the question of whether or not a large number is composite or prime.