

numbers x to $p-1$ into $f(x)$ to find which give $f(x) \equiv 0 \pmod{p}$ ✓

The theorem is not true for composite moduli. For example $x^2 \equiv 1 \pmod{8}$ has $x \equiv 1, 3, 5, 7 \pmod{8}$ as solutions. ✓

There is an analogous extension for congruences into the irrational or complex numbers. $x^2 \equiv 6 \pmod{7}$ has no solutions in the integers $\pmod{7}$, since 6 is a quadratic non residue of 7, but we can adjoin a quadratic non residue to the residues $\pmod{7}$ to give a solution, in the same way as adjoining $\sqrt{2}$ to \mathbb{Z} to give a soln to $x^2 = 2$ in the irrationals, or adjoining i to \mathbb{Z} to give a soln to $x^2 = -4$ in the complex field. ✓

We can describe how to find solutions to the general congruence $f(x) \equiv 0 \pmod{m}$, where m is composite, $m = \prod p_i^{a_i}$ in two stages. ✓

First consider the congruence $f(x) \equiv 0 \pmod{m}$ where $m = \prod p_i^{a_i}$ and the p_i are distinct primes. We break the problem down into the set of congruences $f(x) \equiv 0 \pmod{p_i}$ ①

and solve for each p_i . Each congruence will have $\leq a_i$ solns. We can take any single soln from each congruence to form an n -tuple of solutions, (a_1, \dots, a_n) where a_i is some solution of the congruence $f(x) \equiv 0 \pmod{p_i}$ ✓