\[ x^2 \equiv a \ (p^k) \]

**Case 1** \( p \) odd prime \((\neq 2)\)

**THM 1:** \( x^2 \equiv a \ (p^k) \) has 0 or 2 solutions

**Pf:** \( x^2 \equiv a \ (p) \) has 0 or 2 solutions.
If there is \( d \in \mathbb{Z}_p \) s.t. \( d^2 \equiv a \), then \( x = \pm d \) are the two solutions.
\( d \neq -d \) or else \( 2d = 0 \iff d = 0 \) \( (p \) odd is used here, 2 is invertible) \( a \neq d^2 \) no solutions.

\( x^2 \equiv a \ (p^k) \) use the earlier technique

\( P(x) = x^2 - a \quad P'(x) = 2x \)

\( 2 \Delta \equiv 0 \ (p) \) unless \( \Delta = 0 \). \( \Box \)

**THM 2:** \( p = 2 \) a odd.

(i) \( x^2 \equiv a \ (2) \) has exactly one solution \( a \) odd \( \Rightarrow a = 1 \) solution is \( x = 1 \equiv -1 \)

(ii) \( x^2 \equiv a \ (4) \) has a solution only if \( a \equiv 1 \). \( x = \pm 1 \) or \( x = 1, 3 \)

(iii) \( x^2 \equiv a \ (8) \) has solution only if \( a \equiv 1 \)
(iv) \( k \geq 3 \) \( x^2 = a \ (2^k) \) has solutions only if \( a \equiv 1 \ (\text{mod} \ 8) \). In that case, 4 solutions.

(i) clear

(ii) \[
\begin{array}{c|cccc}
  x & 0 & 1 & 2 & 3 \\
  a = x^2 & 0 & 1 & 0 & 1 & 0
\end{array}
\]
So \( a \equiv 1 \)

TWO SOLUTIONS

(iii) \[
\begin{array}{cccccc}
  x & 0 & \pm 1 & \pm 2 & \pm 3 & \pm 4 \\
  a = x^2 & 0 & 1 & 4 & 1 & 0
\end{array}
\]
So \( a \equiv 1 \)

(iv) \( x^2 - a \equiv 0 \ (2^k) \implies x^2 - a \equiv 0 \ (8) \)
So \( a \equiv 1 \ (\text{mod} \ 8) \)

\[
\begin{align*}
  s^2 & \equiv a \ (\text{mod} \ 2^k) \\
  (\pm s \pm 2^{k-1}) &= \Delta + 2s + 2^{k-2} \implies \Delta^2 \equiv a \ (2^k)
\end{align*}
\]
So we only need to show 

"Exactly 4 solutions"

(i) Odd numbers are exactly the invertible congruences in \( \mathbb{Z}_{2^k} \). So they form \( \mathbb{Z}_{2^k}^* \); there are \( 2^k - 2^{k-1} \) of them."
\( a = 1 + 8 \alpha \cdot 2^{k-3} \) such numbers.

For any \( x \in \mathbb{Z}_2^k \), \( x^2 \equiv 1 \pmod{8} \)

Suppose \( x_1^2 \equiv x_2^2 \pmod{2^k} \)

\((x_1 - x_2)(x_1 + x_2) \equiv 0 \pmod{2^k}\)

\(x_1\) and \(x_2\) assumed odd.

\( \gcd(x_1 - x_2, x_1 + x_2) \) must divide \((x_1 - x_2) + (x_1 + x_2) = 2x_1\)

So at most one power of 2 divides both \((x_1 - x_2)\) and \((x_1 + x_2)\)

\(2^1 \mid (x_1 - x_2)\) \& \(2^1 \mid (x_1 + x_2)\)

But no higher power divides both.

Since \(2^k \mid (x_1 - x_2)(x_1 + x_2)\)

we must have \(2^{k-1} \mid (x_1 - x_2)\) or \(2^{k-1} \mid (x_1 + x_2)\)

Say \(2^{k-1} \mid (x_1 - x_2)\) and \(0 < x_2 < x_1 < 2^k\). We conclude \(x_1 - x_2 = 2^{k-1}\)
Conclusion: \( x_1 = \pm x_2 \) or \( x_1 = \pm x_2 \pm 2^{k-1} \)

at most 4 solutions.

But \( 4 \cdot 2^{k-1} = 2^{k-3} \cdot 2^{k-1} \)

\( a \equiv 1 (8) \) \( x \) odd

number of solutions