SQUARES MODULO PRIMES

When the congruence $a \equiv x^2 \bmod m$ has a solution x, we write $a \equiv \Box \bmod m$ (and say a is a square modulo m).

We will consider the condition $a \equiv \Box \bmod p$ in two ways: first with fixed p and varying a and then with fixed a and varying p.

To begin, with fixed p and varying a, we tabulate all the nonzero squares modulo the primes up to 29:

Mod 2: 1
Mod 3: 1
Mod 5: 1, 4
Mod 7: 1, 2, 4
Mod 11: 1, 3, 4, 5, 9
Mod 13: 1, 3, 4, 9, 10, 12
Mod 17: 1, 2, 4, 8, 9, 13, 15, 16
Mod 19: 1, 4, 5, 6, 7, 9, 11, 16, 17
Mod 23: 1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18
Mod 29: 1, 4, 5, 6, 7, 9, 13, 16, 20, 22, 23, 24, 25, 28

Example. The number 2 is in the list for modulus 7 since $2 \equiv 3^2 \bmod 7$.

Turning things around, we now fix a and list p such that $a \equiv \Box \bmod p$. Actually, we can't list all such p (there are infinitely many primes), but we will work with the primes up to 200. There are 46 such primes:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101,$$

$$103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199.$$

For these primes, we collect them below according to those satisfying $a \equiv \Box \bmod p$ for various choices of a.

Condition: $-1 \equiv \Box \bmod p$
True for $p = 2, 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, 101, 109, 113, 137, 149, 157, 173, 181, 193, 197.$

Condition: $2 \equiv \Box \bmod p$
True for $p = 2, 7, 17, 23, 31, 41, 47, 71, 73, 79, 89, 97, 103, 113, 127, 137, 151, 167, 191, 193, 199.$

Condition: $-2 \equiv \Box \bmod p$
True for $p = 2, 3, 11, 17, 19, 41, 43, 59, 67, 73, 83, 89, 97, 107, 113, 131, 137, 139, 163, 179, 193.$

Condition: $3 \equiv \Box \bmod p$
True for $p = 2, 3, 11, 13, 23, 37, 47, 59, 61, 71, 73, 83, 97, 107, 109, 131, 157, 167, 179, 181, 191, 193.$

Condition: $-3 \equiv \Box \bmod p$
True for $p = 2, 3, 7, 13, 19, 31, 37, 43, 61, 67, 73, 79, 97, 103, 109, 127, 139, 151, 157, 163, 181, 193, 199.$

Condition: $5 \equiv \Box \bmod p$
True for $p = 2, 5, 11, 19, 29, 31, 41, 59, 61, 71, 79, 89, 101, 109, 131, 139, 149, 151, 179, 181, 191, 199.$

Condition: $-5 \equiv \Box \bmod p$
True for $p = 2, 3, 5, 7, 23, 29, 41, 43, 47, 61, 67, 83, 89, 101, 103, 107, 109, 127, 149, 163, 167, 181.$

Example. The prime 7 is in the list for $2 \equiv \Box \bmod p$ since $2 \equiv 3^2 \bmod 7$.