```
oddprimes[n_] := Delete[Table[Prime[i], {i, 1, n + 1}], 1]
```

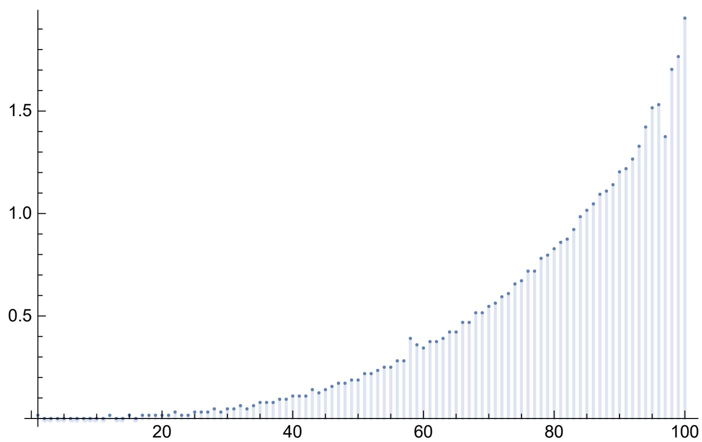
Question : For some prime integers p greater that 2, the equation $x^2 = -1$ has a solution in $\mathbb{Z}_p$. What is the rule that dictates which primes those are?

I know that it depends on the value of p mod 4.

```
check[n_] := Module[{j, k, l, list, square, mod, pairs},
  list = Table[Mod[k^2, oddprimes[n][[j]]] - oddprimes[n][[j]],
    {j, 1, n}, {k, 1, oddprimes[n][[j]]}];
  square = Table[Intersection[{-1}, list[[k]]], {k, 1, n}];
  mod = Table[Mod[oddprimes[n][[j]], 4], {j, 1, n}];
  pairs = Table[Append[square[[j]], mod[[j]]], {j, 1, n}];
  Table[Or[pairs[[k]] == {3}, pairs[[k]] == {-1, 1}], {k, 1, n}]]
check[10]
```

```
{True, True, True, True, True, True, True, True, True, True}
```

```
DiscretePlot[Timing[check[n]][[1]], {n, 1, 100}]
```

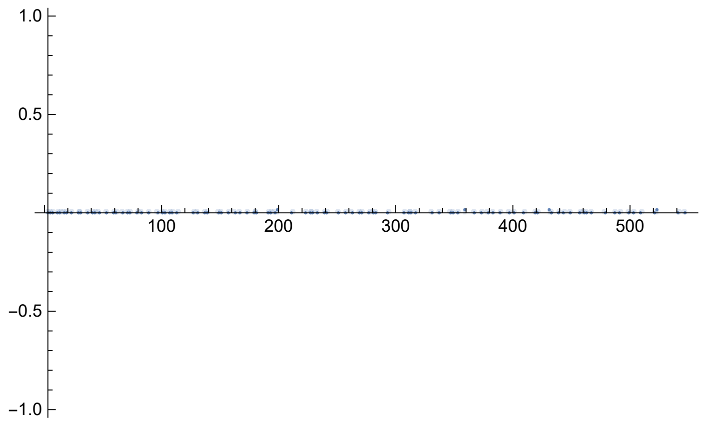


The running time of this algorithm is really bad, mostly because it uses a silly way of checking that -1 is a square.

```
modpair[i_, p_] := {Mod[i^2, p] == p - 1, {i}}
modpairs[p_] := Table[modpair[i, p], {i, 1, p - 1}]
search[p_] := Which @@ Flatten@modpairs[p]
square[p_] := If[TrueQ[search[p] == Null], "is not", "is"]
evidence[p_] := Print ["-1 ", square[p], " a square mod " , p "."]
Table[evidence[p], {p, oddprimes[10]}];
```

```
-1 is not a square mod 3 .

-1 is a square mod 5 .

-1 is not a square mod 7 .

-1 is not a square mod 11 .

-1 is a square mod 13 .

-1 is a square mod 17 .

-1 is not a square mod 19 .

-1 is not a square mod 23 .

-1 is a square mod 29 .

-1 is not a square mod 31 .
```

```
DiscretePlot[Timing[square[n]], {n, oddprimes[100]}]
```



As an output for the demonstration in class :

```
conjecture[p_] :=
 Print ["-1 ", square[p], " a square mod " , p, ", which is ", Mod[p, 4], " mod 4." ]
Table[conjecture[p], {p, oddprimes[10]}];
```

```
-1 is not a square mod 3, which is 3 mod 4.

-1 is a square mod 5, which is 1 mod 4.

-1 is not a square mod 7, which is 3 mod 4.

-1 is not a square mod 11, which is 3 mod 4.

-1 is a square mod 13, which is 1 mod 4.

-1 is a square mod 17, which is 1 mod 4.

-1 is not a square mod 19, which is 3 mod 4.

-1 is not a square mod 23, which is 3 mod 4.

-1 is a square mod 29, which is 1 mod 4.

-1 is not a square mod 31, which is 3 mod 4.
```