In [2]:
```
# determines if a is a quadratic residue of p
def legendre(a, p, d = 2):
    symbol = ((a % p) ** ((p - 1) // d)) % p
    # handles negative -1
    return symbol if symbol < 2 else -1
```

1. Find $[3/2]$, $[-3/2]$, $[\pi]$, $[-7]$, and $[x]$ for $0 \leq x < 1$.

$[3/2]$: 1

$[-3/2]$: -2

$[\pi]$: 3

$[-7]$: -7

$[x]$ for $0 \leq x < 1$: 0

2. With reference to the notation of Theorem 1.2 prove that $q = [b/a]$.

$b = qa + r \Rightarrow q = \frac{b}{a} - \frac{r}{a}$. By the definition of division, $\frac{b}{a} = q + \frac{r}{a}$. Because $0 \leq r < a \implies \frac{r}{a} < 1$, and $q \in \mathbb{Z}$ by identity, $\left\lfloor \frac{b}{a} \right\rfloor = q$.

3. Prove that 3 is a quadratic residue of 13, but a not quadratic nonresidue of 7

We will accomplish this by finding the necessary Legendre symbols.

In [3]:
```
assert legendre(3, 13) == 1
print("3 is a quadratic residue of 13")

assert legendre(3,7) == -1
print("3 is not a quadratic residue of 7")
```

```
3 is a quadratic residue of 13
3 is not a quadratic residue of 7
```

4. Find the values of $\left(\frac{a}{p}\right)$ in each of the 12 cases, $a = -1, 2, -2, 3$ and $p = 11, 13, 17$.

In [4]:
```python
a = [-1, 2, -2, 3]
p = [11, 13, 17]

# print header
out = ""
for i in ["p/a"] + p: out += "{:>3}{}".format(i, " |")
print(out)
print("-" * len(out))

# print rows
for i in a:
    out = ""
    out += "{:>3}{}".format(i, " |")
    for j in p:
        out += "{:>3}{}".format(legendre(i, j), " |")
    print(out)
```

```
p/a | 11 | 13 | 17 |
--------------------
 -1 | -1 |  1 |  1 |
  2 | -1 | -1 |  1 |
 -2 |  1 | -1 |  1 |
  3 |  1 |  1 | -1 |
```

5. Prove that the quadratic residues of 11 are $1, 3, 4, 5, 9,$ and list all solutions of each of the ten congruences $x^2 \equiv a (\mathrm{mod}\ 11)$ and $x^2 \equiv a (\mathrm{mod}\ 11^2)$ where $a = 1, 3, 4, 5, 9$.

In [25]:

```
# hypothesied residues
resd = [1, 3, 4, 5, 9]

# loop through natural numbers lt 11, find residues, compare
# with given values
if [j for j in range(1, 11) if legendre(j, 11) == 1] == resd:
    print("Given values verified!\n")
else:
    print("Math machine broke")

# find solutions of first form (through brute force!)
print("\nFinding solutions of form x ^ 2 = a (mod 11)")
for i in resd:
    print("\nFinding solutions of {}:".format(i))
    for j in range(1, 11):
        if (j ** 2) % 11 == i:
            print("{} ^ 2 = {} mod {}".format(j, i, 11))

print("Done!\n")
# find solutions of second form (through brute force!)
print("\nFinding solutions of form x ^ 2 = a (mod 11 ^ 2)")
for i in resd:
    print("\nFinding solutions of {}:".format(i))
    for j in range(1, 11 ** 2):
        if (j ** 2) % (11 ** 2) == i:
            print("{} ^ 2 = {} mod {} ^ 2".format(j, i, 11))
print("Done!")
```

```
Given values verified!


Finding solutions of form x ^ 2 = a (mod 11)

Finding solutions of 1:
1 ^ 2 = 1 mod 11
10 ^ 2 = 1 mod 11

Finding solutions of 3:
5 ^ 2 = 3 mod 11
6 ^ 2 = 3 mod 11

Finding solutions of 4:
2 ^ 2 = 4 mod 11
9 ^ 2 = 4 mod 11

Finding solutions of 5:
4 ^ 2 = 5 mod 11
7 ^ 2 = 5 mod 11

Finding solutions of 9:
3 ^ 2 = 9 mod 11
8 ^ 2 = 9 mod 11
Done!


Finding solutions of form x ^ 2 = a (mod 11 ^ 2)

Finding solutions of 1:
1 ^ 2 = 1 mod 11 ^ 2
120 ^ 2 = 1 mod 11 ^ 2

Finding solutions of 3:
27 ^ 2 = 3 mod 11 ^ 2
94 ^ 2 = 3 mod 11 ^ 2

Finding solutions of 4:
2 ^ 2 = 4 mod 11 ^ 2
119 ^ 2 = 4 mod 11 ^ 2

Finding solutions of 5:
48 ^ 2 = 5 mod 11 ^ 2
73 ^ 2 = 5 mod 11 ^ 2

Finding solutions of 9:
3 ^ 2 = 9 mod 11 ^ 2
118 ^ 2 = 9 mod 11 ^ 2
```

6. (a) List the quadratic residues of each of the primes $7, 13, 17, 29, 37$.

In [32]:
```python
p = [7, 13, 17, 29, 37]

for i in p:
    print("Quadratic residues of {}:".format(i))
    print(str([j for j in range(1,i) if legendre(j, i) == 1])[1:-1])
    print("")
```

```
Quadratic residues of 7:
1, 2, 4

Quadratic residues of 13:
1, 3, 4, 9, 10, 12

Quadratic residues of 17:
1, 2, 4, 8, 9, 13, 15, 16

Quadratic residues of 29:
1, 4, 5, 6, 7, 9, 13, 16, 20, 22, 23, 24, 25, 28

Quadratic residues of 37:
1, 3, 4, 7, 9, 10, 11, 12, 16, 21, 25, 26, 27, 28, 30, 33, 34, 36
```

(b) For any positive integer n, define $F(n)$ to be the minimum value of $|n^2 - 17x|$, where x runs over all integers. Prove that $F(n)$ is either 0 or a power of 2.

I will be using the '%' symbol to indicate use of the modulo operator.

To find the minimum value as part of $F(n)$, we want to find the value of x which is closest to $\frac{n^2}{17}$. By observation, we see that this makes $F(n)$ very similar to the remainder of $\frac{n^2}{17}$, however we need to keep into account the absolute value of negative modulos. Therefore, we can define $F(n)$ as $min(n^2\%17, n^2 - (n^2\%17))$ which will always be less than $\frac{17}{2}$. Because $\forall x \in \mathbb{Z}, x^2\%17 \in R \cup 0$ where R is the residue class of 17 and $F(n) < \frac{17}{2}$, we can conclude that $F(n) \in \{0, 1, 2, 4, 8\}$.