1.36

Compute the value of $2^{(p-1)/2}$ (mod p) for every prime $3 \leq \text{p} < 20$. Make a conjecture as to the possible values of $2^{(p-1)/2}$ (mod p) when p is prime and prove that your conjecture is correct.

$$2^{(p-1)/2} = r \pmod{\text{p}}$$

Table 1: $3 \leq p < 20$

p	r
3	2
5	4
7	1
11	10
13	12
17	1
19	18

Conjecture: $r \equiv \pm 1$ (mod p) where p is prime.

Proof: Let $r = 2^{(p-1)/2}$. Then $r^2 = 2^{(p-1)}$ by simplification. Since 2 is prime, $p \nmid 2$. Then by Fermat's Little Theorem, $r^2 = 2^{(p-1)} \equiv 1$ (mod p). Thus $x^2 \equiv 1$ (mod p). Now $r \equiv \pm 1$ (mod p) by $1^2 = 1$ and $-1^2 = 1$.