Let p be an odd prime and let m and r be defined by $p-1 = 2^r\, m$ where m is odd. Then

- For all b with $0 < b < p$, $b^{p-1} = 1 \bmod p$. (Fermat)
- For all x with $0 < x < p$, if $x^2 = 1 \bmod p$, then $x = \pm 1 \bmod p$.

From these two facts it follows that, for any fixed b in the range $0 < b < p$,

- **either** $\quad b^m \;=\; 1 \mod p$
- **or** $\quad (b^m)^{2^s} \;=\; -1 \mod p \quad$ for some $0 \le s < r$

Example. Consider $p = 41$. Then $p - 1 = 40 = 2^3\, 5$, so we have $r = 3$, $m = 5$. For a given b, either $b^5 = 1$ or one of b^5, b^{10}, b^{20} is 40 mod 41.

b	b^5	$b^{10} \,\%\, 41$	$b^{20} \,\%\, 41$
1	1	1	1
2	32	40	1
3	38	9	40
4	40	1	1
5	9	40	1
6	27	32	40
7	38	9	40
8	9	40	1
9	9	40	1
10	1	1	1
11	3	9	40
12	3	9	40
13	38	9	40
14	27	32	40
15	14	32	40
16	1	1	1
17	27	32	40
18	1	1	1
19	27	32	40
20	32	40	1
21	9	40	1
22	14	32	40
23	40	1	1
24	14	32	40
25	40	1	1
26	27	32	40
27	14	32	40
28	3	9	40
29	38	9	40
30	38	9	40
31	40	1	1
32	32	40	1
33	32	40	1
34	3	9	40
35	14	32	40
36	32	40	1
37	1	1	1
38	3	9	40
39	9	40	1
40	40	1	1