

a) Suppose $r < 600$ divides $600 = 2^3 \cdot 3 \cdot 5^2$
 then we know that r must be of the form
 $r = 2^{m_1} 3^{m_2} 5^{m_3}$ where $0 \leq m_1 \leq 3$, $0 \leq m_2 \leq 1$, $0 \leq m_3 \leq 2$. Since $r < 600$, $m_1 + m_2 + m_3 < 6$,
 so either $m_1 < 3$, or $m_2 < 1$, or $m_3 \leq 2$.

If $m_1 \leq 2$ then r divides 300.

If $m_2 = 0$ then r divides 200.

If $m_3 \leq 1$ then r divides 120.

Thus we see that any integer less than 600 which divides 600 must also divide at least one of the three numbers 300, 200, and 120.

b) We know that $\text{ord}_{601}(7) < 600$ and divides 600, so by part a $\text{ord}_{601}(7)$ must divide at least one of the numbers: 300, 200, 120.

c) If $\text{ord}_{601}(7)$ divides 300, then $7^{300} \equiv 1 \pmod{601}$ because 300 is a multiple of $\text{ord}_{601}(7)$ and $7^{\text{ord}_{601}(7)} \equiv 1 \pmod{601}$. Similarly if $\text{ord}_{601}(7)$ divides 200 or 120 then that respective power would have to be equivalent to 1 $\pmod{601}$. Since we know that 7^{300} , 7^{200} , and 7^{120} are all not equivalent to 1 $\pmod{601}$ we know that $\text{ord}_{601}(7)$ must not divide 300, 200, or 120.

d) By part c we know that $\text{ord}_{601}(7)$ does not divide 300, 200, or 120, and by part b we know that if $\text{ord}_{601}(7) < 600$ it would have to, thus we see that $\text{ord}_{601}(7)$ must be equal to 600. Thus, by definition 7 is a primitive root of 601.

e) $p-1 = q_1^{a_1} \dots q_s^{a_s}$ where q_i is a prime for $i \in \{1, 2, \dots, s\}$ and each a_i is a natural number.

Suppose $g < p$

Then we know that $\text{ord}_p(g)$ must divide $p-1$

\Rightarrow either $\text{ord}_p(g) = p-1$ or

$\text{ord}_p(g)$ divides one of the numbers:

$$q_1^{a_1-1} q_2^{a_2} \dots q_s^{a_s}, q_1^{a_1} q_2^{a_2-1} \dots q_s^{a_s}, \dots, q_1^{a_1} q_2^{a_2} \dots q_s^{a_s-1}$$

Thus, to check whether or not g is a primitive root, it suffices to calculate:

$$g^{q_1^{a_1-1} q_2^{a_2} \dots q_s^{a_s}} \pmod{p}, g^{q_1^{a_1} q_2^{a_2-1} \dots q_s^{a_s}} \pmod{p}, g^{q_1^{a_1} q_2^{a_2} \dots q_s^{a_s-1}} \pmod{p}.$$

If none of the above are equivalent to 1 \pmod{p} then we know that $\text{ord}_p(g) = p-1$ which means that g is a primitive root of p .