

Q1a: By theorem 6.7c, it is sufficient to check whether 2 is a primitive root of p^2 , for $p \in \{3, 5, 7, 11, 13, 17, 19, 23\}$.

Furthermore, by lemma 6.4, it suffices to show whether or not $2^{\frac{\phi(p^2)}{q}} \neq 1$ in U_{p^2} for q which divide $\phi(p^2)$. We first compute $\phi(3^2) = 6$. This will have prime divisors of 2, 3. Therefore, we have that $2^{\frac{6}{2}} = 2^3 = 8$ which is not 1. Similarly, we have that $2^{\frac{6}{3}} = 2^2 = 4$ which is also not 1. Hence 2 is a generator of U_{3^2} . Next we evaluate $\phi(5^2) = 20$. We see that 2, 5 are prime and divide $\phi(5^2)$. We see that $2^{\frac{20}{2}} = 2^{10} = -1$ and $2^{\frac{20}{5}} = 2^4 = 16$. Neither of these are equal to 1 in U_{5^2} . Next, we see that $\phi(7^2) = 42$. The unique prime divisors of 42 are 2, 3, 7. We can verify that $2^{\frac{42}{2}} = 2^{21} = 1$, so 2 is not a generator of the group U_{7^2} . Next, we compute $\phi(11^2) = 110$. This will have unique prime divisors of 2, 5, 11. One can easily verify that $2^{\frac{110}{2}}, 2^{\frac{110}{5}}, 2^{\frac{110}{11}}$ are not 1 in U_{11^2} . Next, we compute $\phi(13^2) = 156$. This will have unique prime factors of 2, 3, 13. We can easily verify that $2^{\frac{156}{2}}, 2^{\frac{156}{3}}, 2^{\frac{156}{13}}$ are not 1 in U_{13^2} . Next, we compute $\phi(17^2) = 272$. This will have prime divisors of 2 and 17. We can verify that $2^{\frac{272}{2}} = 1$ in U_{17^2} . Therefore, 2 is not a generator of U_{17^2} . Next, $\phi(19^2) = 342$. This will have prime divisors of 2, 3, 19. We see that $2^{\frac{342}{2}}, 2^{\frac{342}{3}}, 2^{\frac{342}{19}}$ are not 1 in U_{19^2} . Finally, we compute $\phi(23^2) = 506$. This will have unique prime factors of 2, 11, 23. We can check that $2^{\frac{506}{2}} = 1$ in U_{23^2} .

Q1b: First we compute $\phi(18)$ as 6. The only prime divisors are 2 and 3. Thus any primitive root a of U_{18} must satisfy $a^2 \neq 1$ and $a^3 \neq 1$ in U_{18} . We can verify using that the only numbers that satisfy this are $5, 11 \in U_{18}$. Similarly, for U_{27} , we compute $\phi(27) = 18$. So any primitive root a of U_{27} must satisfy $a^9 \neq 1$ and $a^6 \neq 1$. The only solutions to this are $2, 5, 11, 14, 20, 23 \in U_{27}$.

Q1ci : If we let $h = g + rp$ for $r \in \{1, 2, \dots, p-1\}$, we have that $h^{p-1} = 1 - rpg^{p-2}$ by the binomial theorem. Furthermore, since r is coprime with p , we have that rpg^{p-2} is not 0 in U_{p^2} . Therefore by lemma 6.2 we have that it is a primitive root. Since this is true for all r , we have that there will be $p-1$ primitive roots in U_{p^2} for each root in U_p .

Q1cii: We can check that $\phi(25) = 20$ which is divisible by 2 and 5. Therefore, we can check that $2^{\frac{20}{2}} \neq 1$ and $2^{\frac{20}{5}} \neq 1$ in U_{25} . hence 2 is a primitive root,