QUESTION
Using you answers to questions 1 and 2, find all solution of the following equations:-
(i) $x^5 \equiv 4 \bmod 27$ (ii) $x^3 \equiv 9 \bmod 187$ (iii) $x^4 \equiv 5 \bmod 18$.
ANSWER

(i) By q.2, a primitive root mod 27 can be chosen, We choose 2 here. (5 would do just as well.) Now 4 can be written as 2^2 mod 27 (or 5^4 if you are using 5 as your primitive root). We may then write $x \equiv 2^k \bmod 27$ (5^k in the other case). The equation then reads $2^{5k} \equiv 2^2 \bmod 27$, i.e. $2^{5k-2} \equiv 1 \bmod 27$. As the order of 2 mod 27 is $\phi(27) = 18$, we obtain $5k - 2 \equiv 0 \bmod 18$, or $5k \equiv 2 \bmod 18$. (If you used 5 as your primitive root, you should have $5k \equiv 4 \bmod 18$ here).

As gcd(5,18)=1, there is a unique root mod 18 to this congruence,which, by using $5k \equiv 2 \equiv 20 \bmod 18$, we can see is 4. Thus $k \equiv 4 \bmod 18$, and there is a unique root to $x^5 \equiv 4 \bmod 27$, namely $2^4 \equiv 16 \bmod 27$ (Using 5 as a primitive root, we get $k \equiv 8 \bmod 18$ and hence arrive at the same conclusion concerning x.)

(ii) $x^3 \equiv 9 \bmod 187$. Now 187=11.17, and as there is no primitive root mod 11.17, we'll begin by solving separately the two congruences $x^3 \equiv 9 \bmod 11$ and $x^3 \equiv 9 \bmod 17$. From question2, 2 is a primitive root mod 11, and by calculating powers of 2 we find that $9 \equiv 2^6 \bmod 11$. We are thus solving $x^3 \equiv 2^6 \bmod 11$, so setting $x = 2^k$ we get $2^{3k} \equiv 2^6 \bmod 11$, or $2^{3k-6} \equiv 1 \bmod 11$. It follows that the order of 2 mod 11 (i.e.10) must divide $3k - 6$, and so we get $3k \equiv 6 \bmod 10$. Since gcd(3,10)=1, this congruence has a unique solution, which we see, on dividing by 3, is $k \equiv 2 \bmod 10$. Thus the only solution of $x^3 \equiv 9 \bmod 11$ is $x \equiv 2^2 \equiv 4 \bmod 11$.

From question 1(iii), 5 is a primitive root mod 17, so this time we write 9 as a power of 5 mod 17. By trial and error (i.e. by calculating powers of 5 mod 17), we find that $9 \equiv 5^{10} \bmod 17$. (Using $9 \equiv -8 \bmod 17$, and the equations $5^8 \equiv -1 \bmod 16$, and $5^2 \equiv 8 \bmod 17$ from question 1 achieves this quickly!) Thus setting $x = 5^k$ our equation now reads $5^{3k} \equiv 5^{10} \bmod 17$, or $5^{3k-10} \equiv 1 \bmod 17$. We may now deduce $3k - 10 \equiv 0 \bmod \phi(17)$, and as $\phi(17) = 16$, this reads $3k \equiv 10 \bmod 16$.

Since gcd(3,16)=1, this congruence has a unique solution which we may obtain, e.g., by multiplying through by 5 to get $-k \equiv 50 \equiv 2 \bmod 16$, so that $k \equiv -2 \equiv 14 \bmod 16$. Thus (using the calculations in question

1), $x \equiv 5^{14} \equiv 5^8.5^4.5^2 \equiv -1.13.8 \equiv -1.-1.8 \equiv 32 \equiv 15 \bmod 17$. Thus the unique solution of $x^3 \equiv 9 \bmod 17$ is $x \equiv 15 \bmod 17$.

If c is a simultaneous solution of $x \equiv 4 \bmod 11$ and $x \equiv 15 \bmod 17$, then $c^3 \equiv 9 \bmod 11$ and $c^3 \equiv 9 \bmod 17$, so that $c^3 \equiv 9 \bmod 187$. Moreover, any root of $x^3 \equiv 9 \bmod 187$ satisfies both $x^3 \equiv 9 \bmod 11$ and $x^3 \equiv 9 \bmod 17$, and so $x \equiv 4 \bmod 11$ and $x \equiv 15 \bmod 17$. By the Chinese Remainder Theorem the two congruences $x \equiv 4 \bmod 11$ and $x \equiv 15 \bmod 177$ have a unique simultaneous solution mod 187, and so the equation $x^3 \equiv 9 \bmod 187$ has a unique solution. If we note that $4 \equiv 15 \bmod 11$, we see that 15 satisfies both congruences, so it is the simultaneous solution we seek. Hence the unique solution of $x^3 \equiv 9 \bmod 187$ is $x \equiv 15 \bmod 187$.

(iii) By question 2, 5 is a primitive element mod 18, and $\phi(18) = 6$. Setting $x \equiv 5^k \bmod 18$, we need to solve $5^{4k} \equiv 5$ mod18, i.e. $5^{4k-1} \equiv 1 \bmod 18$. This gives $4k \equiv 1 \bmod 6$, but as gcd(4,6)=2, which does not divide 1, this congruence has no solutions. Thus $x^4 \equiv 5 \bmod 18$ has no solutions.