MATH342 Feedback and Solutions 7

1. $7^2 \equiv -2 \mod 17$ and $7^3 \equiv -2 \times 7 \equiv 3 \mod 7$. So $7^5 \equiv -6 \mod 17$ and $7^8 \equiv (-2)^4 \equiv -1 \mod 17$. So $7^{13} = 7^5 \times 7^8 \equiv 6 \mod 17$. Since the order of $7 \mod 17$ is a divisor of 16 and $7^8 \equiv -1$ we see that the order of 7 is 16 and $7^x \equiv 6 \Leftrightarrow x \equiv 13 \mod 16$.

In order to know that 13 is the only answer $\mod 16$, *we need to know that 7 is primitive, which follows from* $7^8 \equiv -1 \mod 17$

2.

(i)

$$\phi(22) = \phi(2)\phi(11) = 1 \times 10 = 10.$$

So a primitive root must have order 10. We have

$$7^2 \equiv 5 \mod 22$$

and

$$7^4 \equiv 5^2 \equiv 3 \mod 22.$$

So

$$7^5 \equiv 21 \equiv -1 \mod 22.$$

So 7 is primitive.

To show that 7 is primitive we need to kow that 7 is of order $10 = \phi(22)$, for which it suffices to show that 7 is not of order 2 and 5. By Euler's Theorem, we know that the order of 7 is a divisor of $10 = \phi(22)$.

(ii) If $y^5 \equiv -1 \mod 22$ then either $y \equiv -1 \mod 22$ or y has order 10 and is primitve So $y = 7$ is one solution to $y^5 \equiv -1 \mod 22$. The other primitive ones are y^n where n is coprime to 10, that is,

$$n = 3, \quad 7, \quad 9.$$

These give

$$y \equiv 7^3 \equiv 7 \times 5 \equiv 13 \equiv -9, \quad y \equiv 7^7 \equiv -7^2 \equiv -5, \quad y \equiv 7^9 \equiv -7^4 \equiv -3.$$

So the solutions are

$$-1, \ 7, \ -9, \ -5, \ -3 \mod 22.$$

The solution used above obtains three of the primitive roots are of the form $7^n \mod 22$ *for n coprime to $\phi(22) = 10$: a result proved in lectures. It would also be possible to work through the elements of G_{22}: there are 10 elements but obviously 1 and -1 are not primitive, so that leaves 8: ± 3, ± 5, ± 7, ± 9. None of these elements has order 2 since only $-1 \equiv 21$ has order 2, and in any case this can be checked by direct calculation. The only other possible orders are 5 and 10. Since $(-a)^5 = -a^5$ and $a^5 = \pm 1$ for all $a \in G_{22}$, exactly one of $\pm a$ has order 5, for $a \in \{3, 5, 7, 9\}$ and the other is primitive. So it suffices to compute* $a^5 \mod 22$ *for $a \in \{3, 5, 7, 9\}$, to find all the primitive elements.*

(iii) For any x,

$$19^x \equiv (-3)^x \equiv (-1)^x 3^x \equiv 7^{9x} \mod 22$$

and

$$17 \equiv -5 \equiv 7^7 \mod 22.$$

Now

$$7^{9x} \equiv 7^7 \mod 22 \quad \Leftrightarrow \quad 7^{9x-7} \equiv 1 \mod 22$$

$$\Leftrightarrow 9x \equiv -x \equiv 7 \mod 10 \quad \Leftrightarrow \quad x \equiv (-1) \times 7 \equiv 3 \mod 10.$$

3. *Note that the Miller Rabin test is only applicable to base 2 at level k if $(n-1)/2^k$ is an integer and if $2^{(n-1)/2^i} \equiv 1$* $\mod n$ *for $0 \le i < k$. In particular, in order to apply the test at level k the test needs to be passed at level i for $0 \le i < k$: and more than than this in general.*

Although this was not asked for in the question, those numbers which pass the Miller Rabin test at all levels have been certified prime using Factoris. (One cannot be certain that they are prime, just because they pass the test.) In all the cases given, where the Miller Rabin test fails for n, it fails at level 0, that is, the Fermat test fails. In these cases, the prime factorisation of n has been given using Factoris.

n	level 0 $n-1$ $2^{n-1} \mod n$	level 1 $(n-1)/2$ $2^{(n-1)/2} \mod n$	level 2 $(n-1)/4$ $2^{(n-1)/4} \mod n$	level3 $(n-1)/8$ $2^{(n-1)/8} \mod n$	passes/ factorisation certified
9331	9330 2171	4665 inapplicable	non-integer inapplicable	non-integer inapplicable	$7 \times 31 \times 43$
9337	9336 1	4668 1	2334 1	1267 -1	passes and certified
9341	9340 1	4670 -1	2335 inapplicable	non-integer inapplicable	passes and certified
9343	9342 1	4671 1	noninteger inapplicable	noninteger inapplicable	passes and certified
9347	9346 3377	4673 inapplicable	noninteger inapplicable	noninteger inapplicable	13×719
9353	9352 3036	4676 inapplicable	2338 inapplicable	1169 inapplicable	47×199
9359	9358 4909	4679 inapplicable	noninteger inapplicable	noninteger inapplicable	$7^2 \times 191$
9367	9368 6524	4684 inapplicable	2342 inapplicable	1171 inapplicable	$17 \times 19 \times 29$

4. Since p is prime and $2 < p$, by Fermat's Little Theorem we have $2^{p-1} = 1 \mod p$. So $p \mid 2^{p-1} - 1$ and hence $2 \mid 2(2^{p-1} - 1)$. Since $2(2^{p-1} - 1) = 2^p - 2 = q - 1$, we have $p \mid q - 1$ and $pr = (q - 1)$ for some $r \in \mathbb{Z}$. Then from $2^p \equiv 1 \mod q$ we deduce that $2^{q-1} = 2^pr \equiv 1^r \equiv 1 \mod q$, because the order of 2 modulo q divides p and hence must also divide $q - 1$.

Now if p is and odd prime and $q - 1 = m \times 2^k$ then since p and 2^k are coprime and $p \mid (q - 1)$, we must have $p \mid m$ and, once again, $m = pr$ for some $r \in \mathbb{Z}_+$ and $2^m = 2^{pr} \equiv 1^r \equiv 1 \mod q$.

5.

a) Korselt's Criterion for N to be a Carmichael number, where $N = \prod_{i=1}^{r} p_i^{k_i}$, is: $k_i = 1$ for all i and $p_i - 1 \mid N - 1$ for all i.

b) We have $2465 = 5 \times 493 = 5 \times 17 \times 29$, a product of distinct primes, that is, $k_i = 1$ for $1 \leq i \leq 3$. We also have $N - 1 = 2464 = 8 \times 308 = 8 \times 4 \times 77 = 2^5 \times 7 \times 11$. Since $5 - 1 = 4 = 2^2$ divides 2^5 and $17 - 1 = 2^4$ divides 2^5, and $29 - 1 = 28 = 2^2 \times 7$ divides $2^5 \times 7$, we see that $p_i - 1$ divides $N - 1$ for $1 \leq i \leq 3$. So Korselt's Criterion is satisfied.

c) If $r \geq 2$then p_i is an odd prime for at least one i and $p_i - 1$ is even for at least one i. But then since $p_i - 1 \mid N - 1$, it must be the case that $N - 1$ is even and hence N is odd.

It is possible that $p_1 = 2$, but since N is a composite number, we know that $r \geq 2$ and hence p_i is odd for at least one i and hence $p_i - 1$ is even for at least one i — which is all that is needed.