1) We want to calculate $1234^{7865435}$ mod 11.
Note that $1234 \equiv -1+2-3+4 \pmod{11}$, that is, $1234 \equiv 2 \pmod{11}$.
Since $\gcd(2,11) = 1$ we have $2^{10} \equiv 1 \pmod{11}$. Now
$7865435 = (786543) \cdot 10 + 5$ so
$$2^{7865435} \equiv 2^{(786543) \cdot 10 + 5} \pmod{11} \equiv 2^{10786543} \cdot 2^5 \pmod{11} \equiv 1^{786543} \cdot 2^5 \pmod{11} \equiv 2^5 \pmod{11},$$
and $2^5 = 32 \equiv 10 \pmod{11}$.
Hence, $1234^{7865435} \equiv 10 \pmod{11}$.
It follows that $1234^{7865435} \pmod{11} = 10$.

2) We compute $3^{15}$ mod 10:
Let us first use Fast Modular exponentiation (FME). Write
$15= 8+4+2+1$.
$3^2 = 3 \cdot 3 = 9 \equiv 9 \pmod{10}$
$3^4 = 9 \cdot 9 = 81 \equiv 1 \pmod{10}$
$3^8 = 1 \cdot 1 = 1 \equiv 1 \pmod{10}$
and so $3^{15} = 3^8 \cdot 3^4 \cdot 3^2 \cdot 3^1 = 1 \cdot 1 \cdot 9 \cdot 3 = 27 \equiv 7 \pmod{10}$.
Hence $3^{15} \equiv 7 \pmod{10}$.
To compute $2^{644}$ mod 645 the long way by FME, write $644=512+128+4 = 2^{9} + 2^7 + 2^2$.
By successive squaring and reducing modulo 645 we get
$2^2 = 2 \cdot 2 = 4 \equiv 4 \pmod{645}$
$2^4 = 4 \cdot 4 = 16 \equiv 16 \pmod{645}$
$2^8 = 16 \cdot 16 = 256 \equiv 256 \pmod{645}$
$2^{16} = 256 \cdot 256 = 65,536 \equiv 391 \pmod{645}$
$2^{32} = 391 \cdot 391 = 152,881 \equiv 16 \pmod{645}$
$2^{64} = 16 \cdot 16 = 256 \equiv 256 \pmod{645}$
2^{128} \equiv 256 \cdot 256 = 65,536 \equiv 391 \pmod{645}

2^{256} \equiv 391 \cdot 391 = 152,881 \equiv 16 \pmod{645}

2^{512} \equiv 16 \cdot 16 = 256 \equiv 256 \pmod{645}.

Now \, 2^{644} = 2^{512} \cdot 2^{128} \cdot 2^{4}, \text{ and hence } 2^{644} \equiv 256 \cdot 391 \cdot 16 \pmod{645}.

So 256 \cdot 391 = 100,099 \equiv 121 \pmod{645} \text{ and } 121 \cdot 16 = 1,936 \equiv 1 \pmod{645}. \text{ Hence } 2^{644} \pmod{645} = 1.

3) We first find \, 128^{129} \pmod{17}.

Note that 17 is a prime and 17 does not divide 128. Thus

128^{16} \equiv 1 \pmod{17}. \text{ Now note } 128 = 16 \cdot 8. \text{ Also } 128 \equiv 9 \pmod{17}. \text{ Hence writing}

129 = 128 + 1 = (6 \cdot 128) + 1, \text{ we get}

128^{129} = 9^1 \equiv 9 \pmod{17}.

By Fermat’s Little Theorem, 29^{10} \equiv 7^{10} \equiv 1 \pmod{11}.

Thus, 29^{25} = 7^5 = 7(-4)^4 = 7 \cdot 256 = 7 \cdot 3 = 21 \equiv 10 \pmod{11}.

4) By Fermat’s Little Theorem,

\[ 2^6 \equiv 3^6 \equiv 4^6 \equiv 5^6 \equiv 6^6 \equiv 1 \pmod{7}. \text{ Thus,} \]

\[ 2^{20} + 3^{30} + 4^{40} + 5^{50} + 6^{60} = 2^2 + 3^0 + 4^4 + 5^2 + 6^0 = 4 + 1 + 2^8 + 25 + 1 = 4 + 1 + 4 + 4 + 1 = 14 \equiv 0 \pmod{7}. \]

5) Let \, n \, be a Carmichael number, then we may assume that \, n \, is at least 4. If \, n \, is even, then

\[(n-1)^{n-1} \equiv (-1)^{n-1} = -1 \pmod{n},\]

so \, n \, is not a Carmichael number.

6) Suppose that \, n \, has two prime factors, \, n = pq, \text{ where } p \text{ and } q \text{ are prime, } p \text{ is greater}
than q. Then

(p-1) is greater than (q-1), so (p-1) does not divide (q-1).

Suppose n = p.q. We show that (p-1) divides (n-1) if and only if it divides (q-1).

Indeed q \equiv 1 \mod (q-1) gives n = pq \equiv p \mod (q-1) which implies

n-1 \equiv p-1 \mod (q-1). Since 0 < p-1 < q-1, we see that p-1 is not divisible by q-1.

Hence q-1 cannot divide p-1 as n-1 and p-1 are congruent modulo q-1.

Using this above, we see that (p-1) does not divide (n-1). Similarly q-1 does not divide n-1. A Carmichael number is a pseudoprime to every base b, with the property that (b, n)=1. Let b be such a base, then (b, n) = 1 and (b, p) = (b, q) = 1.

b^(n-1) \equiv 1 \mod n.

It was mentioned in class that if n = p_1 p_2...p_k then n is a Carmichael number if and only if

(k>2) and (p_i -1) divides (n-1). We only proved the \Longrightarrow direction and I mentioned that the converse is true. Hence a Carmichael number has at least three prime factors.