1) It is given to you that $11^6 \equiv 4 \bmod 43$. Find the remainder when 11^{19} is divided by 43.

<u>Ans:</u> We know that if $a \equiv b \bmod m$, then $a^n \equiv b^n \bmod m$ for any natural number n. Additionally $c \cdot a \equiv c \cdot b \bmod m$ for any integer c.

As $11^6 \equiv 4 \bmod 43$, we have that $(11^6)^3 \equiv 4^3 \bmod 43 \Rightarrow 11^{18} \equiv 64 \equiv 21 \bmod 43$. Multiplying 11 to both sides, we see that $11^{19} \equiv 11 \times 21 (= 231) \equiv 16 \bmod 43$. Thus the remainder is 16.

2) It is given to you that $11^6 \equiv 4 \bmod 43$. Find the remainder when 11^{90} is divided by 43.

<u>Ans:</u> As 43 is a prime number and 11 is not divisible by 43, by Fermat's little theorem we have that $11^{42} (= 11^{(43-1)}) \equiv 1 \bmod 43$. Thus $11^{84} (= (11^{42})^2) \equiv 1 \bmod 43 \Rightarrow 11^6 \times 11^{84} \equiv 11^6 \times 1 \bmod 43 \Rightarrow 11^{90} \equiv 11^6 \equiv 4 \bmod 43$. Thus the remainder is 4.

3) Find the remainder when 3^{50} is divided by 15.

<u>Ans:</u> We will explore two ways of doing this.

a) $3^3 (= 27) \equiv -3 \bmod 15 \Rightarrow 3^6 (= (3^3)^2) \equiv (-3)^2 \equiv 3^2 \bmod 15$. We repeatedly use the fact that $3^6 \equiv 3^2 \bmod 15$ by taking suitable powers. If we cube both sides, we get $3^{18} \equiv 3^6 \equiv 3^2 \bmod 15$. Next, we square both sides of the previous equation to get $3^{36} \equiv 3^4 \bmod 15$. Multiply 3^14 on both sides to get $3^{50} \equiv 3^{18} \bmod 15$. But we already know from our previous calculations that $3^{18} \equiv 3^2 \bmod 15$. Thus 3^{50} leaves a remainder of $3^2 = 9$ when divided by 15.

b) $15 = 3 \times 5$. Clearly 3^{50} is divisible by 3. By Fermat's little theorem, $3^4 \equiv 1 \bmod 5$. Taking the 12th power on both sides, we get $3^{48} \equiv 1 \bmod 5$. Thus $3^{50} \equiv 3^2 \equiv 4 \bmod 5$. The remainder modulo 15 must also leave the same remainders as 3^{50} when divided by 3, and 5. Then we must answer the following question : Find r such that $0 \leq r < 15$, and 3 divides r and r leaves a remainder of 4 when divided by 5. The possible choices for r from the second condition are 4, 9, 14. Only one of them is divisible by 3 i.e. 9 which is the answer we are looking for.

4) Find a natural number x such that $11x$ leaves a remainder of 1 when divided by 25.

<u>Ans:</u> We want to solve $11x \equiv 1 \bmod 25$. In other words, we want to find the multiplicative inverse of $\bar{11}$ in the class of remainders modulo 25. First of all, it is necessary that 11 and 25 be coprime for a multiplicative inverse to exist.

Let's use the Euclidean division algorithm to compute the GCD of 11 and 25.
$25 = 11 \times 2 + 3$,

$11 = 3 \times 3 + 2$,
$3 = 2 \times 1 + 1$.

Thus the GCD of 11 and 25 is 1 i.e. they are coprime. We trace the steps backwards to find integers m, n such that $25m + 11n = 1$.
$3 - 2 = 1 \Rightarrow 3 - (11 - 3 \times 3) = 1 \Rightarrow 3 \times 4 - 11 = 1 \Rightarrow (25 - 11 \times 2) \times 4 - 11 = 1 \Rightarrow 25 \times 4 + 11 \times (-9) = 1$. From the equation $25 \times 4 + 11 \times (-9) = 1$, we note that when divided by 25, 11×-9 leaves a remainder of 1. Thus -9 or $25 + (-9) = 16$ is the inverse of 11 modulo 25. We can check by noting that $11 \times 16 = 176$ leaves a remainder of 1 when divided by 25. Thus $x = 16$ is one possible answer. (any natural number in the remainder class of 16 is an answer. For instance $25 + 16(-41), 50 + 16(= 66), 75 + 16(= 91)$,etc.)

5) Find the last two digits of 13^{150}.

<u>Ans:</u> The last two digits of 13^{150} is equal to the remainder r when it is divided by 100. As $100 = 25 \times 4$, 13^{100} and r leave the same remainders when divided by 25, and 4. So we try to compute 13^{150} mod 25 and 13^{150} mod 4 instead.

$13 \equiv 1 \text{ mod } 4$. Thus $13^{150} \equiv 1^{150} \equiv 1 \text{ mod } 4$.

$13^2 \equiv 19 \equiv -6 \text{ mod } 25$. Squaring both sides, we get $13^4 \equiv 36 \equiv 11 \text{ mod } 25 \Rightarrow 13^8 \equiv 11^2 \equiv 21 \equiv -4 \text{ mod } 25 \Rightarrow 13^{16} \equiv (-4)^2 \equiv 16 \text{ mod } 25$. Thus $13^4 \times 13^{16} \equiv 11 \times 16 \equiv 1 \text{ mod } 25$. Once we have $13^{20} \equiv 1 \text{ mod } 25$, by taking 7th power on both sides, we get $13^{140} \equiv 1 \text{ mod } 25$. This implies that $13^{150} \equiv 13^{10} \text{ mod } 25$. Also using our previous calulations, we get $13^{10} = 13^8 \times 13^2 \equiv (-4) \times (-6) \equiv 24 \text{ mod } 25$. We conclude that $13^{150} \equiv 24 \text{ mod } 25$.

Thus we also have that $r \equiv 1 \text{ mod } 4$ and $r \equiv 24 \text{ mod } 25$. As $0 \leq r < 100$, from the second part, we have that r must be one of the following: $24, 49, 74, 99$. Only one of the above numbers, 49, leaves remainder 1 when divided by 4. Thus $r = 49$.

6) For a RSA cipher, if the two primes are $p = 17, q = 19$, find two valid candidates for e (encoding power) and d (decoding power) such that neither of them is equal to 1. (In other words, find non-trivial ones.)

<u>Ans:</u> Our encoding power, e, must be co-prime to $(p - 1)(q - 1) = (17 - 1) \times (19 - 1) = 16 \times 18 = 288$. We choose $e = 7$. The decoding power d has the property that $e \cdot d$ leaves a remainder of 1 when divided by $m = (p - 1)(q - 1)$. So, we need to find the multiplicative inverse of 7 modulo 288.

$288 = 7 \times 41 + 1$. Thus the multiplicative inverse of 7 is $288 + (-41) = 247$. Thus we have $d = 247$ as the decoding power.

7) We have a RSA cipher based on the two primes $p = 5, q = 7$ and $e = 11$. If $A \to 01.B \to 02, \cdots, Z \to 26$, what is the encrypted version of the message "EXAM"? (Note that the encrypted version is a string of numbers all of which are less than 35.)

Ans: EXAM $\to$ 05 24 01 13. We use the encoding power (11) to raise the numbers to the power 11 and store the remainders modulo $p \cdot q = 5 \times 7 = 35$.

E translates as 5^{11} mod 35.
$5^2 \equiv -10 \bmod 35 \Rightarrow 5^4 \equiv (-10)^2 \equiv -5 \bmod 35 \Rightarrow 5^8 \equiv (-5)^2 \equiv 5^2 \bmod 35 \Rightarrow 5^2 \times 5^8 = 5^{10} \equiv 5^2 \times 5^2 \equiv 5^4 \equiv -5 \bmod 35 \Rightarrow 5^{11} \equiv 5 \times -5 \equiv 10 \bmod 35$. Thus the encoding of E is 10.

X translates as 24^{11} mod 35.
$24 \equiv -11 \bmod 35 \Rightarrow 24^2 \equiv (-11)^2 \equiv 121 \equiv 16 \bmod 35 \Rightarrow 24^4 \equiv 16^2 \equiv 11 \bmod 35 \Rightarrow 24^8 \equiv 11^2 \equiv 16 \bmod 35 \Rightarrow 24^2 \times 24^8 = 24^{10} \equiv 16 \times 16 \equiv 11 \bmod 35 \Rightarrow 24 \times 24^{10} = 24^{11} \equiv (-11) \times 11 \equiv -121 \equiv 19$. Thus the encoding of X is 19.

A translates as 1^{11} mod 35. Thus the encoding of A is 01.

M translates as 13^{11} mod 35.
$13^2 \equiv -6 \bmod 35 \Rightarrow 13^4 \equiv (-6)^2 \equiv 36 \equiv 1 \bmod 35 \Rightarrow 13^8 \equiv 1 \bmod 35 \Rightarrow 13^2 \times 13^8 = 13^{10} \equiv (-6) \times 1 \equiv -6 \bmod 35 \Rightarrow 13^{11} \equiv 13 \times (-6) \equiv -78 \equiv -8 \equiv 27 \bmod 35$. Thus the encoding of M is 27.

The encrypted message reads as 10 19 01 27.

8) Note that $11 \times 11 \equiv 1 \bmod 24$. In the previous question with $p = 5, q = 7$ we have that $(p-1)(q-1) = 24$. Thus the decoding power is also 11. Check that the encrypted message is the correct one.

Ans: We decode 10 19 01 27 using the decoding power which is coincidentally also 11.

Translate 10 to 10^d mod 35. $(d = 11)$
$10^2 \equiv -5 \bmod 35 \Rightarrow 10^4 \equiv 25 \equiv -10 \bmod 35 \Rightarrow 10^8 \equiv (-10)^2 \equiv -5 \bmod 3510^2 \times 10^8 = 10^{10} \equiv (-5) \times (-5) \equiv 25 \equiv -10 \bmod 35 \Rightarrow 10^{11} \equiv -100 \equiv 5 \bmod 35$. Thus 10 is decrypted as 05 which is indeed correct.

Compute $19^d \bmod 35, 1^d \bmod 35, 27^d \bmod 35$ and check that the results are $24, 01, 13$ respectively.