On RSA

The reason $\phi(N) = (p-1)(q-1)$

$\phi(x)$ is a function that returns the number of integers less than x that are coprime to x (they share no prime factors). For example:

$$\phi(3) = 2$$

$$\boxed{1 \quad 2} \quad 3$$

$$\phi(7) = 6$$

$$\boxed{1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6} \quad 7$$

Generaly, where p is a prime: $\phi(p) \equiv p - 1$ because p is coprime to all the positive integers lower than it and there are $x - 1$ positive integers less than x.

$$\phi(p) \equiv p - 1$$

$$\underbrace{1\ 2\ 3\ \ldots}_{p-1 \text{ numbers}} \quad p$$

$$\phi(7 \times 3)$$

$$\begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & \boxed{7} \\ 8 & 9 & 10 & 11 & 12 & 13 & \boxed{14} \\ 15 & 16 & 17 & 18 & 19 & 20 & \end{array}$$

$$\boxed{\text{multiple of 7}} \quad \boxed{\text{multiple of 3}}$$

This is the grid for $\phi(7)$ with an aditional 3 rows. Notice that all the multiples of 7 are in the last column and there is a single multiple of 3 in each column. This means that for each coprime to 7, there are 2 less than 21 that are also coprime to 3 (numbers coprime to 3 and 7 are coprime to 21).

on Euclid's algorithm Euclid's algorithm finds the Greatest Common Divisor (GCD) of 2 numbers. If the GCD of 2 numbers is 1, then they are coprime. The result of a division is given as quotient "r" remainder. For example, to find $GCD(50, 15)$

$$\frac{50}{15} = 3 \text{ r } 5$$

$$\frac{15}{\underbrace{5}_{\text{GCD}}} = 3 \text{ r } 0$$

When the remainder is 0, the divisor of the last division is the greatest common divisor so $GCD(50, 15) = 5$

Or, to find $GCD(50,13)$

$$\frac{50}{13} = 3 \text{ r } 11$$

$$\frac{13}{11} = 1 \text{ r } 2$$

$$\frac{11}{2} = 5 \text{ r } 1$$

$$\frac{2}{\underbrace{1}_{\text{GCD}}} = 2 \text{ r } 0$$

$$GCD(50,13) = 1 so 50 \text{ and } 13 \text{ are coprimes}$$

on prime factorisation
To break RSA we must find the prime factors of N.