Prime Numbers

Prime number is simply a no. that has only 2 factors: one and itself

Relatively Prime

Two numbers are Relatively Prime if they share no common factor other than 1.
e.g.$_1$/ 38 & 55 {neither is prime} but factors of 38: 1 , 2, 19
factors of 55: 1 , 5 , 11 → nos are Rel. Prime
e.g.$_2$/ 22,55 are not {common factor:11}

Some Exponential Identities:

$X^a \,.\, X^b = X^{(a+b)}$

=

$(X^a)^b = X^{(a.b)}$

$m^{(p-1)} \text{ mod } p = 1$ {that is what Fermat discovered !} where p is a prime number and m < p

e.g.$_1$/ $7^{10} \text{ mod } 11 = 1$

Euler Function:

If $\boldsymbol{n = p \,.\, q}$ and p , q are prime numbers → $m^{(p-1)(q-1)} \text{ mod } n = 1$

e.g./ p =11 , q = 5 → n = 55 & $(p-1)(q-1) = 40$ → $38^{40} \text{ mod } 55 = 1$

(in this case, we don't need to compute anything).

But to let this work: m, n must be relatively prime. (Note: 38, 55 are relatively prime in this e.g.)

Now, by multiplying both sides by m: $m \,.\, m^{(p-1)(q-1)} \text{ mod } n = 1 \,.\, m$

Therefore, $m^{(p-1)(q-1)+1} \text{ mod } n = m$ (get back to m)

i.e. we can raise m to some power and the result is m !

That is to say $m^{\phi(n)+1} \text{ mod } n = m$ *(so, we can perform some operations, and end up with what we started !).*

Back to our e.g./: p =11 , q = 5 → n = 55 & *(p-1)(q-1) = 40 → so, what is for e.g.* 7^{42} *mod 55?*

Ok. …. $7^3 = 7^2 \times 7 = 49 \times 7 = 343 = 13 \bmod 55$

$7^4 = 7^3 \times 7 = 13 \times 7 = 91 = 36 \bmod 55$

:

7^{40} = … *don't compute….we know it's 1 (Euler fn.)*

i.e. $7^{40} = 1 \bmod 55$

then $7^{41} = 1 \times 7 = 7 \bmod 55$

Then the final answer is : $7^{42} = 49 \bmod 55$

Finding Primes:

To find large prime number:

1- *Find a random number*
2- *Make sure it's odd (all primes other than 2 are odd numbers)*
3- *Perform the Fermat Tests, and see if passes the test !*
4- *If not, add 2 and go to step 3*

e.g./ suppose you have following random number: 116 (even number, so add 1)

117/3 = 39(not a prime) {so we can eliminate117 and every 3 no. after117: ~~117~~,~~120~~,~~123~~..

Now, 117+2 = 119 {divide by 3,5,7} → 119/7 = 17 {not a prime} {so eliminate every no, divisible by 7}

121 by 3, 5, 7, 11 …… 121/11 = 11

121 + 2 = 123 (divide by 3)

123 + 2 = 125 (divide by 5) so eliminate 130, 135,…

125 + 2 = 127 (not divisible by 3,5,7, or 11}

Fermat Test:

$m^{(p-1)} \bmod p = 1 \rightarrow m^p \bmod p = m$

but if p is not prime, the answer will not be m

Note: 3^6 mod 6 = 3 (m)   however, 6 is not a prime and passes the Fermat test (since 3 < mod 6)

Also, 5^6 mod 6 = 1(not 5) → that is to say: 6 is not a prime

So, to make sure that the number is prime you need to run Fermat test more than on time:

FT1 : find 2^rmod r → if answer not equal 2, then r is not a prime: go to FT2

FT2: find 3^rmod r → if answer not equal 2, then r is not a prime: go to FT3, FT5, and FT7.

Then we can say it is a prime

Back to our e.g./

2^{127} mod 127 = 2 ✓

3^{127} mod 127 = 3 ✓

5^{127} mod 127 = 5 ✓

7^{127} mod 127 = 7 ✓

Well, now you can say it is a prime

Finding the inverse (The Extended Euclidian Algorithm)

To generate RSA key pair, you must be able to find d such that :

e.d =1 mod (p-1)(q-1)

i.e.   d = inverse of e mod (p-1)(q-1)

e.g./   we have a no. say 7 and modulus say 40

so, what is d such that 7 x d = 1 mod 40 ?

1- *Create 2 cols as follows :*

40	40
7	1

2- *Do some simple multiplications and subtractions on both cols.*
   On the second row: multiply 7 by 5 (which is close to the first row)
   2^{nd} row becomes :   35   5
   Subtract 2^{nd} row from 1^{st} one:

5	35

Now we have:

~~40~~	~~40~~
7	1
5	35

Repeat the process:

~~40~~	~~40~~	
7	1	
5	35	
2	-34	
1	103	now you stop

But 103 is greater than modulus: 103 mod 40 = 23

Therefore 23 is the inverse of 7 mod 40:

$$7 \times 23 \bmod 40 = 161 \bmod 40 = 1$$

e.g.$_2$: what is d such that 3 x d = 1 mod 40 ?

40	40
3	1
1	27 ➔ inverse is 27