Prime Numbers

Definition : ——————————————————————————————————

An integer $p > 1$ is a prime number if and only if its only divisors are ± 1 and $\pm p$, and we define P the set of all primes.

Property :

any integer $a > 1$, it exist p repectively in P , for which $p|a$

Proof :

any integer $a > 1$, we take the set of dividor of a $D = \{d|a, 1 < d \leqslant a\}$ the set is not empty it contains a. because D is bounded and include in $\mathbb{Z}$, the minimum of D exist, and we take $d = \min D$, d cant be divisible by anything else rather then $\pm d$ and ± 1 because if it is suppose that it exist $c < d$ for which $c|d$ that will implie that $c|a$ which contradict the fact that d is the minimum of D, so d is divisible just by $\pm d$ and ± 1, hence d is prime.

Property :

any integer $a > 1$, a can be writen as $a = p_1 \times p_2 \times \ldots \times p_t$ with $p_t \leqslant \ldots \leqslant p_1$

Proof :

any integer $a > 1$, if a is prime we are done, if not we use the previous property, it exist p_1 in P and $m_1 > 1$, with $a = m_1 \times p_1$, that give us $m_1 < a$ and p_1, if m_1 is prime we are done if not we do the same thing, it exist p_2 in P and $m_2 > 1$, with $m_1 = m_2 \times p_2$, that give us $m_2 < m_1 < a$ and $p_2 \leqslant p_1$, if we continue like this we have two scenarios stoping at m_k that is prime or have the following result

$m_{k-1} = m_k \times p_k$ with $1 < m_k < \ldots < m_2 < m_1 < a$ and $p_k \leqslant \ldots \leqslant p_2 \leqslant p_1$

this sequence can't continue for ever beacuse its bounded and decrementing, meaning that it exist t for which m_t is the limit of this sequence, and second the limit must be prime because $m_t > 1$ and it will have no other divider becaus if it has we still need to go to $t+1$ which contradict the fact that t is the limit hence we will have

$m_t = p_t$ with $1 < m_t < \ldots < m_2 < m_1 < a$ and $p_t \leqslant \ldots \leqslant p_2 \leqslant p_1$ after a rearengement of the multiplication we donne until we got m_t

a can be expressed as $a = p_1 \times p_2 \times \ldots \times p_t$ with $p_t \leqslant \ldots \leqslant p_2 \leqslant p_1$

Property :

any integer $a > 1$, a can be uniquely written as $a = p_1^{\alpha_{p_1}} \times p_2^{\alpha_{p_2}} \times \ldots \times p_t^{\alpha_{p_t}}$ with $p_t < \ldots < p_1$

Proof :

any integer $a > 1$, can be written as $a = p_1^{(0)} \times p_2^{(0)} \times \ldots \times p_n^{(0)}$ with $p_n \leqslant \ldots \leqslant p_1$, let have the

set of all prime that devid a, $K_1 = \{p \in P,\ p|a\}$, the set is not empty because a is decomposition of primes, and the set is bounded so maximum exist, we take $p_1 = \ max K_1$ we do $p_1|a$, it will give us $b_1 = p_1|a$ with $\alpha_{p_1} = 1$, if there is no p_1 we take the next step if not, we continue until we eliminate all p_1 we get $b_{k_1} = p_1^{(1)} \times \dots \times p_{n-k_1}^{(1)}$ and $\alpha_{p_1} = k_1$, after this we get $K_2 = k_1 - \{p_1\}$ the set of prime devid a that doesnt contain p_1, and $K_2 \subset K_1$, the set is also bounded so we take $p_2 = maxK_2$ we can notice here that $p_2 < p_1$, and we will repeat the same process untill we have $K_{t+1} = \varnothing = K_1 - \{p_1, p_2, \dots p_t\}$, with $p_t < \dots < p_1$ and $K_{t+1} \subset \dots \subset K_2 \subset K_1$, first we are shure that K_{t+1} is empty because every k we take p_k from K_k the set is finit so we will eventualy have an empty set, and second we alwas take $maxK_k$ so $maxK_{k+1} < maxK_k$, so that will give the set $\{(p_1, \alpha_{p_1}), (p_2, \alpha_{p_2}), \dots, (p_t, \alpha_{p_t})\}$, that conatin the accurence of each p_k so we can form a using the set in the following form $a = p_1^{\alpha_{p_1}} \times p_2^{\alpha_{p_2}} \times \dots \times p_t^{\alpha_{p_t}}$ with $p_t < \dots < p_1$.
Next to prove the unicity, let assum that a can be written in two diffrent ways $a = p_1^{\alpha_{p_1}} \times p_2^{\alpha_{p_2}} \times \dots \times p_t^{\alpha_{p_t}}$ and $a = q_1^{\alpha_{q_1}} \times q_2^{\alpha_{p_2}} \times \dots \times q_t^{\alpha_{q_t}}$ that means $p_i^{\alpha_{p_i}}|a$ hence it exist j for which mean $p_i^{\alpha_{p_i}}|q_j^{a_{p_j}}$ so that implies $\alpha_{p_i} \leqslant a_{p_j}$, because q_j and q_i are primes and unique in a, it means that $p_i = q_j$, this statement can be shown first if $p_i|a$ it must exist q_j that equal p_i because we know that we can construct a from q_j's wich will make p_i doesnt devid a wich contradict the fact $p_i|a$, and for the α_{p_i} if we have that q_j and $\alpha_{p_i} > \alpha_{q_i}$ we will get that $p_i^{\alpha_{p_i}}$ contradict the fact that $p_i^{\alpha_{p_i}}|a$, we have $q_j^{a_{p_j}}|a$ means that it must devid $p_i^{\alpha_{p_i}}$ so $a_{p_j} \leqslant \alpha_{p_i}$ which implies $\alpha_{p_i} = a_{p_j}$, beacuse we chose i and j to be arbitrery, hence a can be written in unique form $a = p_1^{\alpha_{p_1}} \times p_2^{\alpha_{p_2}} \times \dots \times p_t^{\alpha_{p_t}}$ with $p_t < \dots < p_1$

Theorem :
Fermat's Theorem states that, for p a prime number, any integer a relativly prime to p verify :
$a^{p-1} \equiv 1 \bmod p$

Proof :
for p a prime number, and a an integer relativly prime to p, lets consider the set $X = \{a \bmod p,\ 2a \bmod p, \dots,\ (p-1)a \bmod p\}$, first we observe that all the element inside X are nonzero, because a is relativly prime to p and all the multiplicative k are in the set $\{1, \dots, p-1\}$ so ak is always relativly prime to p, hence there is no zero element inside X, second we see that all element are unique, let assume that it exist $1 \leqslant k < j < p$, for which $ak \equiv aj \bmod p$, because a is relativly prime to p, a has an inverse so we can remove a from both side, will give us $k \equiv j \bmod p$ which is imposible since k and j are strictly difrent and the both in the set $\{1, \dots, X\}$ hence each element in X is unique, we can now say safely that X is the set $\{1, \dots, p-1\}$ where element have diffrent order, because we have all X element is $ak \bmod p$ and ak is relatively prime to p, and each element is unique and we have $p-1$ elememt so its cover the full set $\{1, \dots, p-1\}$, so we can have the next equality

$(a \bmod p \times 2a \bmod p \times \ldots \times (p-1)a \bmod p) \equiv (1 \times \ldots \times p-1) \bmod p$
we will use mod *arithmetics the result will be*
$a^{p-1}(p-1)! \equiv (p-1)! \bmod p$, *and because* $(p-1)!$ *is relatively prime to p we can remove it from both side and obtain* $a^{p-1} \equiv 1 \bmod p$ *which is the ferma theorem*

Function:
Euler's Totient Function $\phi(n)$ *defined as the number of positive integers less than n and relatively prime to n. By convention,* $\phi(1) = 1$

Property:
if p is a prime number, $\phi(p) = p-1$

Proof:
if p is a prime number, any integer $0 < k < p$ *is relatively prime with p so*

Property
if p and q are two prime number, then $\phi(p \times q) = \phi(p) \times \phi(q)$

Proof:
for p and q two prime number, we take the set of all integer verify $0 < k < pq$ *as* $S = \{1, \ldots, pq-1\}$, *we notice that two major set that there element can devid pq, the first one* $X = \{p, 2p, \ldots, (q-1)p\}$ *and second* $Y = \{q, 2q, \ldots, (p-1)q\}$, *thoes two set represent all the integer that can devid pq because p and q are prime so p is divisble only by p and q only by q, the size of X is* $q-1$ *and the size of Y is* $p-1$, *where S is* $pq-1$ *so we substruct the sets that divise pq we will get all the number that relatively prime to pq so:*

$$
\begin{aligned}
\phi(pq) = \ pq - 1 - ((q-1) + (p-1)) &= \ pq - q - p + 1 \\
&= \ q \times (p-1) - (p-1) \\
&= \ (q-1) \times (p-1) = \phi(q) \times \phi(p)
\end{aligned}
$$

Property:
Any ingeter a relatively prime to n then a mod *n is relatively prime to n*

Proof:
for integer a relatively prime to n, by the euclidiant division, it exist positive integer q for which $a = qn + a \bmod n$ *with* $0 \leqslant a \bmod n < n$, *let* $d = gcd(a, n)$ *and* $e = gcd(n, a \bmod n)$, *then* $d|a$ *and* $d|n$ *then* $d|a - qn = a \bmod n$ *meaning that* $d \leqslant e$, $e|n$ *and* $e|a \bmod n$ *then* $e|qn + a \bmod n = a$, *mean* $e \leqslant d$, *hence* $gcd(a, n) = gcd(n, a \bmod n) = 1$

Theorem:
Euler's theorem states that for every a and n that are relatively prime: $a^{\phi(n)} \equiv 1 \bmod n$

Proof:

for any integer a relatively prime to n, we know that Euler's Totient Function $\phi(n)$ give the number of positive integers less than n and relatively prime to n, so we take the set of thoes integers as $X = \{x_1, \ldots, x_{\phi(n)}\}$, all are relatively prime to n, then we multiply x_i by a and take $\bmod n$ of the result we defined the set, $S = \{ax_1 \bmod n, \ldots, ax_{\phi(n)} \bmod n\}$ we notice two things, first there are no zero elements, because a and x_i are both relatively prime to n so $gcd(ax_i, n) = 1$, and second all the element are distinct, suppose that it exist, $1 \leqslant i < j < \phi(n)$ for which $ax_i \bmod n = ax_j \bmod n$, because $gcd(a, n) = 1$ we can remove a from both side, that give us $x_i \equiv x_j \bmod n$ which is impossible because x_i and x_j are less then n and relatively prime with n, contradiction, meaning all the element are distinct inside S, we resume two thing S have no zero element, and all element are distinct prime to n and because S has $\phi(n)$ element that are distinct we can safely say that S is a purmutation of X, so we can have the following

$(ax_1 \bmod n \times \ldots \times ax_{\phi(n)} \bmod n) \equiv (x_1 \times \ldots \times x_{\phi(n)}) \bmod n$

$a^{\phi(n)} \times \left(\prod_{i=1}^{\phi(n)} x_i\right) \equiv \left(\prod_{i=1}^{\phi(n)} x_i\right) \bmod n$, the number $\left(\prod_{i=1}^{\phi(n)} x_i\right)$ is relatively prime to n, because all x_i are relatively prime to n, $gcd\left(\left(\prod_{i=1}^{\phi(n)} x_i\right), n\right) = 1$ so we can eleminate it from both sides, hence

$a^{\phi(n)} \equiv 1 \bmod n$

---

1) for p a prime number, any integer a verify $a^p \equiv a \bmod p$

Proof:

we state first the case where $a = kp$ for $k \in \mathbb{Z}$ and this is always true, now for the case where $a \neq kp$, it means a is relatively prime to p so we can apply the ferma theorem $a^{p-1} \equiv 1 \bmod p$, we multiply both side with $a \bmod p$, we obtain $a^{p-1} \times a \equiv (1 \times a) \bmod p$, hence $a^p \equiv a \bmod p$

2) for every a and n that are relatively prime: $a^{\phi(n)+1} \equiv a \bmod n$

Proof:

we state first the case where $a = kn$ for $k \in \mathbb{Z}$ and this is always true, now for the case where $a \neq kn$, it means a is relatively prime to n so we can apply the Euler theorem $a^{\phi(n)} \equiv 1 \bmod n$, we multiply both side with $a \bmod n$, we obtain $a^{\phi(n)} \times a \equiv (1 \times a) \bmod n$, hence $a^{\phi(n)+1} \equiv a \bmod n$