

Big O is a set, i.e. a category. $10n = O(n)$ is a shortcut for $10n \in O(n)$. We know that $10n$ is in the category of functions shaped like n .

Likewise, $10n^3 + 75n^2 - 5200n + 1000007$ is in the category of functions shaped like n^3 , so it is $O(n^3)$.

Formally:

$$O(g(n)) = \{f(n) | \exists c, n_0 > 0 \wedge f(n) \leq c \bullet g(n), \forall n > n_0\}$$

Modular exponentiation: $2^{25 \bmod 20} = 2^5 = 32 \bmod 20 = 12$

```

Data: x, y, N
Result:  $x^{y \bmod N}$ 
if  $y = 0$  then
  | return 1;
end
z = modexp( $x, \lfloor \frac{y}{2} \rfloor, N$ );
if  $y$  is even then
  | return  $z^2 \bmod N$ ;
end
else
  | return  $x \bullet z^2 \bmod N$ ;
end

```