Integer Functions

Floor and Ceilings: floor and ceiling function, which are defined for all real x as follows:

$\lfloor x \rfloor =$ the greatest integer less than or equal to x

$\lceil x \rceil =$ the least integer greater than or equal to x

For example, if x = 2.73, then $\lceil x \rceil = 3$ and $\lfloor x \rfloor = 2$. Again, $\lceil -x \rceil = -2$ and $\lfloor -x \rfloor = -3$

MOD: The quotient of n divided by m is $\lfloor n/m \rfloor$, when m and n are positive integers. And the reminder is called 'n mod m'. The basic formula is

$n = m\lfloor n/m \rfloor + n \bmod m$

$\Rightarrow n \bmod m = n - m\lfloor n/m \rfloor$, for $m \neq 0$

See this Chapter from Scanned Class Lecture, *NOT* from Here

For example,

$5 \bmod 3 = 5 - 3\lfloor 5/3 \rfloor = 5 - 3\times 1 = 2$

$5 \bmod -3 = 5 - (-3)\lfloor 5/(-3) \rfloor = 5 + 3\times(-2) = -1$

$-5 \bmod 3 = -5 - 3\lfloor -5/3 \rfloor = -5 - 3\times(-2) = 1$

$-5 \bmod -3 = -5 - (-3)\lfloor -5/(-3) \rfloor = -5 + 3\times 1 = -2$

The number after 'mod' is called the *modulus*, the value of $n \bmod m$ is between 0 and m.

$0 \leq n \bmod m < m$, for $m > 0$

$0 \geq n \bmod m > m$, for $m < 0$

In order to avoid division by zero, we can define $x \bmod 0 = x$.

Distributive law is mod's most important algebraic property. We have

$c(x \bmod y) = (cx) \bmod (cy)$

We can prove this law from definition

$c(x \bmod y) = c(x - y\lfloor x/y \rfloor) = cx - cy\lfloor cx/cy \rfloor = cx \bmod cy$

Divisibility: n is divisible by m, if $m > 0$ and the ration n/m is an integer i.e.

$m \backslash n \Leftrightarrow m > 0$ and $n = mk$ for some integer k.

The *greatest common divisor* (gcd) of two integers m and n is the largest integer that divides them both: $\gcd(m,n) = \max\{k \mid k \backslash m \text{ and } k \backslash n\}$

For example, $\gcd(12,18) = 6$.

Another familiar notion is the *least common multiple* (lcm) can be defined as follows:
$lcm(m,n) = \min\{k \mid k > 0, m \backslash k \text{ and } n \backslash k\}$.

For example, lcm(12,18) = 36.

Gcd is easy to compute using 2300 year old Euclidian algorithm. To calculate gcd(m,n), for given values $0 \le m < n$, Euclid's algorithm uses the following recurrence
$\gcd(0,n) = n$
$\gcd(m,n) = \gcd(n \bmod m, m)$, for $m > 0$

For example, gcd(12,18) = gcd(6,12) = gcd(0,6) = 6.

We can extend Euclid's algorithm so that it will compute integers m' and n' satisfying
$m'm + n'n = \gcd(m,n) \quad \cdots \quad (1)$.
Again, we can let $r = n \bmod m$ and apply the method recursively with r and m in place of m and n which generates new integer $\bar{r}$ and $\bar{m}$
$\bar{r}r + \bar{m}m = \gcd(r,m)$.

Since $r = n - \lfloor n/m \rfloor m$ and $\gcd(r,m) = \gcd(m,n)$, this equation tells us that
$\bar{r}(n - \lfloor n/m \rfloor m) + \bar{m}m = \gcd(m,n)$
$\Rightarrow \bar{r}n - \lfloor n/m \rfloor \bar{r}m + \bar{m}m = \gcd(m,n)$
$\Rightarrow (\bar{m} - \lfloor n/m \rfloor \bar{r})m + \bar{r}n = \gcd(m,n) \quad \cdots \quad (2)$

Now equating equation (1) with equation (2), we get
$n' = \bar{r}$
$m' = \bar{m} - \lfloor n/m \rfloor \bar{r}$

For example, if m = 12 and n = 18, then this method gives the following result.
$6 = 0 \times 0 + 1 \times 6 = 1 \times 6 + 0 \times 12 = (-1) \times 12 + 1 \times 18$

Theorem: $k \backslash m$ and $k \backslash n \Leftrightarrow k \backslash \gcd(m,n)$.
Proof: If k divides both m and n, it divides $m'm + n'n$, thus it divides $\gcd(m,n)$. Conversely, if k divides $\gcd(m,n)$, it divides a divisor of m and a divisor of n, so it divides both m and n.

☺Good Luck☺