**Theorem 1: Divisibility with 3 in base 10.** A natural number is divisible with 3 if and only if the sum of its base10-digits is divisible with 3.

**proof.** Lets say $n = d_0 + d_1 * 10^1 + d_2 * 10^2 + .... + d_k * 10^k$ in base 10, with digits $d_i \in \{0, 1, 2..., 9\}$. That is the same as writing $n = \sum_{i=0}^{k} d_i 10^i$

Recall that modulo 3 means remainder at division with 3. For example 100 mod 3 = 1, because 100=3*33+1.
Also recall that modulo distributes over sum, product, and powers. For example
(100+22) mod 3 = ((100 mod 3) + (22 mod 3)) mod 3.
See the appendix for a recap of modulo operations.

So now we can write:

$n \mod 3 = (\sum_{i=0}^{k} d_i 10^i) \mod 3$
$= (\sum_{i=0}^{k} (d_i 10^i \mod 3)) \mod 3$
$= (\sum_{i=0}^{k} (d_i \mod 3) * (10^i \mod 3)) \mod 3$
$= (\sum_{i=0}^{k} (d_i \mod 3) * (10 \mod 3)^i) \mod 3$
$= (\sum_{i=0}^{k} (d_i \mod 3) * 1^i) \mod 3$
$= (\sum_{i=0}^{k} (d_i \mod 3)) \mod 3$
$= (\sum_{i=0}^{k} d_i) \mod 3$

Reading the beginning and the end in english : The remainder of $n$ divided by 3 is the same as the reminder of the sum-of-digits($n$) divided by 3. In particular if one of these remainder is 0 (that means divisible with 3) the other one is aslo 0.
This is a proof in both directions since we didnt use implications (unidirectional), we used equality modulo 3, which goes both ways.

**Theorem 2: Divisibility with 3 in base 2.** A natural number is divisible with 3 if and only if the alternating sum of its base2-digits is divisible with 3. That is if $n = b_k b_{k-1} ... b_2 b_1 b_0$ in binary then divisibility by 3 comes down to whether the alternating bits sum $+b_0 - b_1 + b_2 - b_3 + ... + (-1)^k b_k$ is divisible by 3.

**proof.** Lets write $n = b_0 + b_1 * 2^1 + b_2 * 2^2 + .... + b_k * 2^k$ in base 2, with digits $b_i \in \{0, 1\}$. That is the same as writing $n = \sum_{i=0}^{k} b_i 2^i$

Repeating the idea in the previous proof, we can write equalities modulo 3:

$n \mod 3 = (\sum_{i=0}^{k} b_i 2^i) \mod 3$
$= (\sum_{i=0}^{k} (b_i 2^i \mod 3)) \mod 3$
$= (\sum_{i=0}^{k} (b_i \mod 3) * (2^i \mod 3)) \mod 3$
$= (\sum_{i=0}^{k} (b_i \mod 3) * (2 \mod 3)^i) \mod 3$
$= (\sum_{i=0}^{k} (b_i \mod 3) * (-1)^i \mod 3) \mod 3$
$= (\sum_{i=0}^{k} b_i * (-1)^i \mod 3) \mod 3$
$= (\sum_{i=0}^{k} (-1)^i b_i) \mod 3$
$= (+b_0 - b_1 + b_2 - b_3 + ... + (-1)^k b_k) \mod 3$

We used here the fact that
$2 \mod 3 = 2 = -1 \mod 3$
which is due to $-1 = -1 * 3 + 2$. The rest of the explanation goes like in the previous proof.

**appendix: modulo arithmetic recap** All numbers here are integers. The integer division of $a$ at $n > 1$ means finding the unique quotient $q$ and remainder $r \in \mathbf{Z}_n$ such that
$a = nq + r$
where $\mathbf{Z}_n$ is the set of all possible remainders at $n$ : $\mathbf{Z}_n = \{0, 1, 2, 3, ..., n-1\}$.

"mod $n$" = *remainder at division with* $n$ for $n > 1$ ($n$ it has to be at least 2)
"$a \mod n = r$" means mathematically all of the following :
· $r$ is the remainder of integer division $a$ to $n$
· $a = n * q + r$ for some integer $q$
· $a, r$ have same remainder when divided by $n$
· $a - r = nq$ is a multiple of $n$
· $n \mid a - r$, a.k.a $n$ divides $a - r$

EXAMPLES
21 mod 5 = 1, because 21 = 5*4 +1
same as saying 5 | (21 − 1)

24 = 10 = 3 = -39 mod 7 , because 24 = 7*3 +3; 10=7*1+3; 3=7*0 +3; -39=7*(-6)+3. Same as saying
7 | (24 − 10) or
7 | (3 − 10) or
7 | (10 − (−39)) etc

**LEMMA** two numbers $a, b$ have the same remainder mod $n$ if and only if $n$ divides their difference.
We can write this in several equivalent ways:
· $a \mod n = b \mod n$, saying $a, b$ have the same remainder (or modulo)
· $a = b(\mod n)$
· $n \mid a - b$ saying $n$ divides $a - b$
· $a - b = nk$ saying $a - b$ is a multiple of $n$ ($k$ is integer but its value doesnt matter)
EXAMPLES
$21 = 11 \text{ (mod 5)} = 1 \Leftrightarrow 5 \mid (21 - 11) \Leftrightarrow 21 \mod 5 = 11 \mod 5$
$86 \text{ mod } 10 = 1126 \text{ mod } 10 \Leftrightarrow 10 \mid (86 - 1126) \Leftrightarrow 86 - 1126 = 10k$
**proof:** EXERCISE. Write "$a \mod n = r$" as equation $a = nq + r$, and similar for $b$

**modulo addition** $(a+b) \mod n = (a \mod n + b \mod n) \mod n$
EXAMPLES
17 + 4 mod 3 = (17 mod 3) + (4 mod 3) mod 3 = 2 + 1 mod 3 = 0

**modulo multiplication** $(a \cdot b) \mod n = (a \mod n \cdot b \mod n) modn$
EXAMPLES
17 * 4 mod 3 = (17 mod 3) * (4 mod 3) mod 3 = 2 * 1 mod 3 = 2

**modulo power** is simply a repetition of multiplications
$a^k$ mod $n$ = ($a$ mod $n$ * $a$ mod $n$ ... * $a$ mod $n$ ) mod $n$

EXAMPLE: $13^{100} \mod 11 =$?
$13 \mod 11 = 2$
$13^2 \mod 11 = 2^2 \mod 11 = 4$
$13^4 \mod 11 = (13^2 \mod 11)^2 \mod 11 = 4^2 \mod 11 = 16 \mod 11 = 5$
$13^8 \mod 11 = (13^4 \mod 11)^2 \mod 11 = 5^2 \mod 11 = 25 \mod 11 = 3$
$13^{16} \mod 11 = (13^8 \mod 11)^2 \mod 11 = 3^2 \mod 11 = 9$
$13^{32} \mod 11 = (13^{16} \mod 11)^2 \mod 11 = 9^2 \mod 11 = 4$
$13^{64} \mod 11 = (13^{32} \mod 11)^2 \mod 11 = 4^2 \mod 11 = 5$
$13^{100} = 13^{64} \cdot 13^{32} \cdot 13^4 \mod 11 = (5 * 4 * 5) \mod 11 = 25 * 4 \mod 11 = 25$
$\mod 11 * 4 \mod 11 = 3 * 4 \mod 11 = 1$