DIVISIBILITY USING MODULO N

Link to: physicspages home page.

To leave a comment or report an error, please use the auxiliary blog and include the title or URL of this post in your comment.

Post date: 6 September 2025.

A couple of useful theorems about the modulo n relation are:

Theorem 1. *Let $n \in \mathbb{N}$ and $a,b,c,d \in \mathbb{Z}$. If $a \equiv c \mod n$ and $b \equiv d \mod n$ then $(a+b) \equiv (c+d) \mod n$ and $(ab) \equiv (cd) \mod n$.*

Theorem 2. *Let $n \in \mathbb{N}$ and $a,b \in \mathbb{Z}$. If $a \equiv b \mod n$ then $a^k \equiv b^k \mod n$ $\forall\, k \in \mathbb{N}$.*

Example 1. Show that $2^{48}-1$ is divisible by 97. We need to show that

$$2^{48} \equiv 1 \mod 97 \tag{1}$$

We begin by finding the largest power of 2 less than 97. This is $2^6 = 64$. Since $97-64=33$ we have

$$2^6 \equiv -33 \mod 97 \tag{2}$$

Using Theorem 2, we therefore have

$$2^{48} = \left(2^6\right)^8 \tag{3}$$

so

$$2^{48} \equiv (-33)^8 \mod 97 \tag{4}$$

We can break this up since $(-33)^8 = \left(33^2\right)^4$ so

$$2^{48} \equiv \left(33^2\right)^4 \mod 97 \tag{5}$$

Now

$$33^2 = 1089 = 97 \times 11 + 22 \tag{6}$$

so

$$33^2 \equiv 22 \mod 97 \tag{7}$$

and

$$2^{48} \equiv 22^4 \mod 97 \tag{8}$$

$$\equiv \left(22^2\right)^2 \mod 97 \tag{9}$$

Then we have

$$22^2 = 484 = 5 \times 97 - 1 \tag{10}$$

833	$= 416 \times 2 + 1$
416	$= 208 \times 2$
208	$= 104 \times 2$
104	$= 52 \times 2$
52	$= 26 \times 2$
26	$= 13 \times 2$
13	$= 6 \times 2 + 1$
6	$= 3 \times 2$
3	$= 2 \times 1 + 1$

TABLE 1. Successive divisions of the exponent.

so

$$22^2 \equiv (-1) \mod 97 \tag{11}$$

Substituting back into 9 we have

$$2^{48} \equiv (-1)^2 \mod 97 \tag{12}$$

$$2^{48} \equiv 1 \mod 97 \tag{13}$$

as required.

It's questionable if this method is easier than just using software to calculate $\frac{2^{48}-1}{97} = 2901803883615$, although if all you have available is a 10-digit calculator, it does provide a way of finding divisibility without have to use any very large numbers.

Example 2. Find $41^{833} \mod 100$. The number 41^{833} is huge, so attempting to calculate this by brute force is difficult. We can break down the calculation by successive divisions (with remainders) of the exponent. We have Table 1.

Starting from bottom and working upwards, we have Table 2.

The integer 41^{833} has 1344 digits, so trying to calculate the mod 100 value using an ordinary calculator is impossible. The calculation in Table 2 never uses any number larger than $41^3 = 68921$.

41^2	$= 1681$	$\equiv 81 \mod 100$	
41^3	$= 41^2 \times 41$	$\equiv 81 \times 41 \mod 100$	$\equiv 21 \mod 100$
41^6	$= \left(41^3\right)^2$	$\equiv 21 \times 21 \mod 100$	$\equiv 41 \mod 100$
41^{13}	$= \left(41^6\right)^2 \times 41$	$\equiv 41 \times 41 \times 41 \mod 100$	$\equiv 21 \mod 100$
41^{26}	$= \left(41^{13}\right)^2$	$\equiv 21 \times 21 \mod 100$	$\equiv 41 \mod 100$
41^{52}	$= \left(41^{26}\right)^2$	$\equiv 41 \times 41 \mod 100$	$\equiv 81 \mod 100$
41^{104}	$= \left(41^{52}\right)^2$	$\equiv 81 \times 81 \mod 100$	$\equiv 61 \mod 100$
41^{208}	$= \left(41^{104}\right)^2$	$\equiv 61 \times 61 \mod 100$	$\equiv 21 \mod 100$
41^{416}	$= \left(41^{208}\right)^2$	$\equiv 21 \times 21 \mod 100$	$\equiv 41 \mod 100$
41^{833}	$= \left(41^{416}\right)^2 \times 41$	$\equiv 41 \times 41 \times 41 \mod 100$	$\equiv 21 \mod 100$

TABLE 2. Calculating $41^{833} \mod 100$.