

Exercises in Modulo Arithmetic

If a divides b without a remainder, we write $a|b$. Ex: 3 divides 9, so $3|9$. 4 does not divide 9, so $4 \nmid 9$.

We say $a \equiv b \pmod{n}$ if $n|(a - b)$. Ex: $5 \equiv 2 \pmod{3}$ because $3|(5-2)$.

We say that a is congruent to b modulo n if $a \equiv b \pmod{n}$. In the above example, 5 is congruent to 3 modulo 2. We can deduce several facts from the modulo relationship.

For example, suppose $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$. Then $n|(a - a')$ and $n|(b - b')$, so $n|(a - a' + b - b') = a + b - (a' + b')$, or $a + b \equiv a' + b' \pmod{n}$. Similarly, $a - b \equiv a' - b' \pmod{n}$. Ex: $5 \equiv 1 \pmod{4}$ and $3 \equiv -1 \pmod{4}$, and $5 + 3 = 8 \equiv 0 = 1 + (-1) \pmod{4}$.

A similar result can be shown with multiplication, that is $ab \equiv a'b' \pmod{n}$. However, this is not always true with division. Ex: $10 \equiv 4 \pmod{6}$, but $\frac{10}{2} = 5 \not\equiv 2 = \frac{4}{2} \pmod{6}$.

How is this useful? Modulo arithmetic can be used to calculate remainders of divisions. Ex: What is the remainder of 3^{99} when divided by 10? note that $3^2 = 9 \equiv -1 \pmod{10}$, so $3^{99} = 3^{2 \cdot 49} * 3 \equiv 9^{49} * 3 \equiv (-1)^{49} * 3 \equiv -3 \pmod{10}$.

1. What is the remainder of 10^{20} when divided by 13?
2. January 1, 2009 is a Thursday. What is October 1, 2009?
3. Prove: if $9|k$, then 9 divides the sum of digits of k . Ex: $9|297$, and $9|2 + 9 + 7 = 18$.
4. The supersum of a number n is the result of repeatedly taking the sum of digits of n until you get a single digit. For example, the supersum of 199240 is the supersum of $1+9+9+2+4+0 = 25$, and the supersum of 25 is 7, thus the supersum of 199240 is 7. What is the supersum of 2^{64} ?
5. Prove: for any number n, m there is a number k such that $n \equiv k \pmod{m}$ where $0 \leq k \leq m - 1$.
6. Prove: if p is prime, then if $p \nmid n$ there is a number m such that $p|nm - 1$.
7. Prove: if p is prime, then $p|(p-1)! + 1$, where $n! = n * (n-1) * \dots * 2 * 1$.