Modular Arithmetic

The Philomath Club

Introduction to Modular arithmetic

- What happens when we divide two integers?
- We get a quotient and a remainder.

The equation looks like-

- A is the dividend
- B is the divisor
- Q is the quotient
- R is the remainder.

$$\frac{A}{B} = \text{Q Remainder } R$$

- ➔ Sometimes we only want to find the remainder.
- ➔ For that we use an operation called the modular operation.
- ➔ As shown in the previous example, we call it A mod B=R
- ➔ Example- 14/5=10 remainder 4
- ➔ So 14 mod 5=4

The clock example

- In a 12-hour clock, the day is divided into 2 periods of 12 hour each.
- If the time is 6:00 now, after 8 hours it will be 14:00

  but it “wraps” every 12 hours. So the time according the 12-hour clock is 2:00.

- We can calculate this faster by modular arithmetic as 14 is congruent to 2 mod 12.

Few Examples

1) What is 8 mod 4?
   (Visualize a 4 hour clock with 0,1,2,3)

2) Find 9 mod 2

3) What is -5(mod 3)?

Euclid's Division lemma

This lemma says that

Dividend=divisor x quotient+remainder.

Try out a few examples and verify yourself.

According to Euclid's Division Lemma if we have two positive integers a and b, then there exist unique integers q and r which satisfies the condition $a = bq + r$ where $0 \leq r < b$.

- So by the previous lemma, if we have A mod B and we increase it by another multiple of B, we have the same remainder.

$$A \bmod B = (A + K.B) \bmod B$$

For example:

3 mod 10=3

13 mod 10 = 10.1+3 = 3

33 mod 10 = 10.3+3 = 3

Congruence Modulo

We use a symbol which looks like this- ≡, which basically means “equivalent”.(three horizontal lines).

A ≡B (mod C)

So 89 ≡ 5 (mod 6)

93 ≡ 3 (mod 9)

Modular addition and subtraction

1. If $a \equiv b \pmod{N}$ then $a + k \equiv b + k \pmod{N}$
2. If $a \equiv b \pmod{N}$, $c \equiv d \pmod{N}$ then $a + c \equiv b + d \pmod{N}$
3. If $a \equiv b \pmod{N}$, then $ka \equiv kb \pmod{N}$ for any integer k
4. If $a \equiv b \pmod{N}$ and $c \equiv d \pmod{N}$, then $ac \equiv bd \pmod{N}$.
5. If $a \equiv b \pmod{N}$, then $a^k \equiv b^k \pmod{N}$ for any positive integer k.
6. If $\gcd(k, N) = 1$ and $ka \equiv kb \pmod{N}$, then $a \equiv b \pmod{N}$

Some Problems

1. Find the sum of 31 and 148 in modulo 24.

2. Find the remainder when 123 + 234+ 32+ 56+ 22 + 12 + 78 is divided by 3.

3. What is (18x6) mod 7?

4. Find the remainder when 124·134·23·49·235·13 is divided by 3.

5. What is 3^16 mod 4?

6. Aditya is excited for his birthday party on Saturday, March 2, 2013. He is turning 16 years old. What day of the week was Aditya born?

7. Ashley went to the movies nine days ago. If Thursdays are the only day of the week that Ashley goes to the movies, then what day of the week is today?

Challenge Problem:

What is the remainder when 6^6^6 is divided by 7

Thank you!