MODULAR ARITHMETIC

Modular Arithmetic is a system of arithmetic involving congruent integers A and B plus a wrap around number set referred to as modulus n. Its modern definition was first introduced by Carl F. Gauss in 1801 and reads-

$$A \equiv B (\text{mod } n)$$

Once given mod(n), B can be determined from A/n=quotient plus remainder B. So, for instance,-

$$17 \equiv 5(mod\ 12)$$

This means 17 hours , as expressed in military language , is equivalent to 5pm civilian time. The modulus 12 represents the twelve hours used in the wrap-around.

By simple substitution one also has-

$$A \equiv B(mod\ n) \quad equals \quad B \equiv A(mod\ n)$$

and the addition and multiplication results-

$$(A+C) \equiv (B+D)\ (\text{mod } n) \qquad (A*C) \equiv (B*D)(mod\ n)\ .$$

With the above modular results we are now free to work out solutions to certain modular equations and also quickly determine the last(or lasr two) digits appearing in a large number.

Lets begin. Consider first finding x for-

$$123 \equiv x \text{ mod}(60)$$

So 123/60=2 plus 3 remainder 3. This produces the solution $123 \equiv 3\ mod(60)$

Next consider-

$$x \equiv (13 + 6*7)\ (\text{mod } 8)$$

Here $13 \to 5, 42 \to 2$, so x=5+2=7.

It is possible to quickly determine the last two digits of a large number by using lmod 100. Thus we can ask what are the two lowest digits appearing in –

N=(24*13*7)^2=4769856

Using ModularArithmetic we have (24*91)^2(mod 100).This can be written as (2184^2 mod(100)=84^2=7056. From this we indeed have that 56 are the last two digits in N.

A really large number is-

N=2419^3714

Let us find the last digit in this integer. We have 2419 mod(10) which leaves us with a remainder of 9^3714=(-1)^3714. But -1 to an even power is +1. Hence the last integer in N will be 1. Amazing how easy Modular Arithmetic can establish the last digit. We point out that mod(1) yields the lowest digit, mod(100) the last two digits and mod(1000) the last three digits of a large number.

Finally let us look at a division problem involving large numbers. Consider the integer quotient

Q=6^113/7;

What will be the last digit in this quotient? Looking at the equivalent form

N=6^113 mod(7)

we find B=(-1)^113=-1 or +6. So the last digit in Q will be 6. The actual working out the entire number for Q by my computer leads to the 88 digit long answer-

121897066235553329411896292709666958612449639501516546008580695963134922294609573179743086 .

Note the 6 ending agrees with the much easier way using Modular Arithmetic. The procedure only works as long as Q terminates without leaving any remaining fraction in its output. So Q=12356/9=1372.8888… fails.

U.H.Kurzweg
June 25, 2024
Gainesville, Florida