Applications of Congruences

Hashing functions: we're all familiar with hash functions from Data structures. Essentially a hash function h: {any string} $\longrightarrow$ {fixed length}.

We can make a simple hash fcn on all integers

$$h(n) = n \bmod m$$

$$h: \mathbb{Z} \to \mathbb{Z}_m$$

we have certain requirements for hash fcns, in particular it must be easy to compute.

However hash functions cannot be 1-to-1. They are always functions from infinite inputs to finite outputs.

When two inputs return the same output we call that a collision.

There are numerous ways to resolve collisions.

Hash functions are nice for databases, don't search all text, (could be long.) just the hash. They are also essential in computer security, i.e., not storing pass words or speeding up computations on keys etc.

Pseudo random numbers: Many applications require randomness, However since we are using computers which are told exactly how to generate said numbers the best we can do is pseudo random.

The simplist pseudo random number generator is defined by 4 ints: modulus m, multipliers a, increment c, & seed x_0 then:

$$x_{n+1} = (a \cdot x_n + c) \bmod m$$

This will appear to behave randomly, though it can be solved for in a closed form.

Ex: Find the sequence of pseudorandom numbers with $m=9$, $a=7$, $c=4$, $x_0=3$

$x_1 = 7x_0 + 4 \bmod 9 = 7 \cdot 3 + 4 \bmod 9 = 25 \bmod 9 \equiv 7$

$x_2 = 7 \cdot 7 + 4 \bmod 9 = 53 \bmod 9 = 8$

$x_3 = 7 \cdot 8 + 4 \bmod 9 = 60 \bmod 9 = 6$

$\vdots$

$x_8 = 7 \cdot 4 + 4 \bmod 9 = 32 \bmod 9 = 5$

$x_9 = 7 \cdot 9 + 4 \bmod 9 = 34 \bmod 9 = 3$

Since we've reached x_0 & every term only depends on previous term $\Rightarrow$ repeats!

3, 7, 8, 6, ..., 5, 3, 7, 8, 6, ...

Cryptography: First classic crypto, Caesar cipher:

This method encrypts messages by shifting letters, modulo 26.

In Caesars case he shifted by 3

$f(p) = (p+3) \bmod 26$ $\quad A \to D \quad B \to E \quad C \to F \quad \dots \quad Z \to C$

Ex Encrypt ATTACK AT DAWN

first we can write this as numbers

0 19 19 0 2 10 0 19 3 0 22 13

Shift by 3:

3 22 22 3 5 13 3 22 6 3 25 16

Convert back:

D W W D F N D W G D Z Q