Previously in Math 103a:

Division algorithm: $a = bq + r, \quad b > 0, \quad 0 \le r < b$

$(\Rightarrow a \bmod b = r)$

If $a_1 \bmod b = r_1$ & $a_2 \bmod b = r_2$, then

$$(a_1 + a_2) \bmod b = (r_1 + r_2) \bmod b$$

&

$$(a_1 a_2) \bmod b = (r_1 r_2) \bmod b$$

Examples!

Ex 1. $a_1 = 10$, $a_2 = 11$, $b = 4$. Find $(a_1 + a_2) \bmod b$

Soln: $10 \bmod 4 = 2$ $\quad [10 = 2 \times 4 + 2]$

$11 \bmod 4 = 3$

$(10+11) \bmod 4 = 5 \bmod 4 = 1$

Since $10 \bmod 4 + 11 \bmod 4 = 5$

& $5 \bmod 4 = 1$.

Ex 2 a_1, a_2, b as in Ex 1. Find $(a_1 a_2) \bmod b$

Soln: $(a_1 a_2) \bmod b = (10 \bmod 4)(11 \bmod 4) \bmod 4$

$= (2)(3) \bmod 4 = 2$

Ex 3. Suppose $a \bmod b = 1$. Find $a^n \bmod b$

Soln: $a^n \bmod b = 1^n \bmod b = 1 \quad (b > 1)$

In particular $10^n \bmod 9 = 1 \quad \forall n$

Ex 4. For $a = 4322$, $b = 27$, find $a \bmod b$.

$a = (4 \times 10^3) + (3 \times 10^2) + (2 \times 10) + 2$

Need to find $10^3 \bmod 27$ & $10^2 \bmod 27$

not the easiest way!

$1 \bmod 27 = 1$

$10 \bmod 27 = 10$

$100 \bmod 27 = 19$, since $100 = 3 \times 27 + 19$

$1000 \bmod 27 = 190 \bmod 27 = 1$

$\therefore 4322 \mod 27 = (4\times1 + 3\times19 + 2\times10 + 2\times1) \mod 27$

$= (4 - 24 \quad -7 + 2) \mod 27$

$= (-31 + 85) \mod 27$

$= (-25) \mod 27$

$= 2$

Application: Check digits

Identification numbers usually have many digits. To catch mistakes when such numbers are copied, an extra digit, called the check digit may be added.

Ex. Suppose ID number = 367412.
If it is copied with one digit wrong, we want the computer to know there is a mistake.
e.g. suppose copied as 397412.

To do this, add an extra digit
e.g. $367412 \mod 9 \quad (=5)$

New ID number is 3674125
↑ check digit

Suppose, instead, the number is entered as 3974125. Since 397412 mod 9 = 8,

this number cannot be an ID number.

Note: An easy way to calculate mod 9:

$$397412 = 3\times10^5 + 9\times10^4 + 7\times10^3 + 4\times10^2 + 1\times10 + 2\times1$$

$$\therefore 397412 \bmod 9 = (3+9+7+4+1+2) \bmod 9$$

$$= 8$$

mod 9 is/was used by USPS as check digit.

Airlines, UPS, some car rental firms use mod 7.

However, neither method can detect all errors of one wrong digit.

Universal Product Code (UPC) uses a different type of check digit, and detects one wrong digit. (and most transposition errors)

Start with 11 digit #

$a_1\ a_2\ a_3\ a_4\ a_5\ a_6\ a_7\ a_8\ a_9\ a_{10}\ a_{11}$

$a_1 a_2 a_3 a_4 a_5 a_6$ identifies manufacturer

$a_7 a_8 a_9 a_{10}$ identifies product

The UPC check digit a_{12} is determined by setting the following dot product to 0:

$$(a_1, a_2, \ldots, a_{12}) \cdot (3, 1, 3, 1, \ldots, 3, 1) \bmod 10 = 0$$

If a_i & a_{i+1} are transposed (but no other mistake is made), then error is **not** detected

$\iff$ $(3a_{i+1} + a_i) \bmod 10 = (3a_i + a_{i+1}) \bmod 10$

$\iff$ $(2a_{i+1}) \bmod 10 = (2a_i) \bmod 10$

$\iff$ $2(a_{i+1} - a_i) \bmod 10 = 0$

$\iff$ $a_{i+1} - a_i$ is a multiple of 5

$\iff$ $|a_{i+1} - a_i| = 5$ ← error detection fails!

since $-9 \le a_{i+1} - a_i \le 9$

More on check digits later in course!

For error detection + correction, need 2 check digits

More properties of integers

We all believe:

Well ordering principle: Every non empty set of positive integers has a smallest element.

Not true for sets of positive rational numbers.

Ex: $S = \{$ all positive rational numbers $\}$ has no smallest element.

Greatest Common Divisor (gcd)

Def: The gcd of two nonzero integers a, b (written $\gcd(a,b)$) is the largest integer dividing both a & b

Ex $\gcd(6, 15) = 3$

Def. a & b are relatively prime if $\gcd(a,b) = 1$

Important Theorem (gcd is a linear combination)

If a, b are nonzero integers, then there exist (nonunique) integers s & t such that $as + bt = \gcd(a,b)$

Corollary If a, b are relatively prime, then $\exists$ s,t such that

$$as + bt = 1$$

In particular, if c is any integer, then $\exists$ s', t' s.t. $as' + bt' = c$.