Corrected
1/9/12

AO

Course website:

www.math.ucsd.edu/~lrothsch/math103a

Integers

Definitions we all know:

(i) t is a divisor of s if $\exists$ u with $s = tu$
written $t|s$

(ii) A positive integer n is prime if n and 1 are its only divisors.

(iii) s is a multiple of t if $\exists\, u$ s.t. $s = tu$

Basic tool: Division (or Euclidean) algorithm

Let a, b integers, $b > 0$. Then $\exists!$ q & r s.t. $\boxed{0 \leq r < b \;\&\; a = bq + r.}$

Note: $\exists!$ means "there exists unique"

Description of algorithm:

Assume $a \geq 0$. (Always have $b > 0$.)

If $a - b < 0$, put $q = 0$ & $r = a$
[$a - b < 0$, $a \geq 0 \Longrightarrow 0 \leq a < b$] done.

If $a - b \geq 0$, check $a - 2b$.

If $a - 2b < 0$, put $q = 1$ & $r = a - b$
[$a - 2b < 0 \Longrightarrow a - b < b$] done.

If $a - 2b \geq 0$, check $a - 3b$

If $a-3b<0$, put $q=2$ & $r=a-2b$ done

If $a-3b\geq 0$, continue... Process ends when reach smallest $\ell>0$ for which

$a-\ell b<0$ $(\Leftrightarrow 0\leq a-(\ell-1)b<b)$

Then put $q=\ell-1$ & $r=a-(\ell-1)b$

Need to check that process ends:

Since $b>0$, $\ell b\geq \ell$, so $a-\ell b\leq a-\ell$

$a-\ell b\geq 0 \Rightarrow a-\ell\geq 0 \Rightarrow a\geq \ell$

impossible to have $a\geq \ell$ $\forall \ell$

Process must end!

Similar algorithm for $a<0$. Find it!

Uniqueness of q & r:

If $a=q_1b+r_1=q_2b+r_2$, need to check $r_1=r_2$ & $q_1=q_2$. WLOG assume $r_2\geq r_1$

Then $r_2-r_1=(q_1-q_2)b$ *

Since $r_2<b$, $r_2-r_1<b$ & $0\leq r_2-r_1<b$

* $\Rightarrow$ b divides r_2-r_1, so $r_2-r_1=0$,

$0=(q_1-q_2)b$, $b>0 \Rightarrow q_2=q_1$ //

Note: In the text, a different proof of the existence of q & r is given.

Ex 1. $a = 14$, $b = 5$ go through algorithm.

$14 - 5 \geq 0$, check $14 - 2\times 5$

$14 - 2\times 5 = 14 - 10 = 4 \geq 0$ check $14 - 3\times 5$

$14 - 3\times 5 = -1 < 0$

$\therefore$ $q = 2$, $r = 14 - 2\times 5 = 4$

Ex 2. $a = -14$, $b = 5$ start with $\ell = -1$

$-14 - (-1)5 = 9 < 0$ try $\ell = -2$

$-14 - (-2)5 = -4 < 0$ Try $\ell = -3$

$-14 - (-3)5 = 1 \geq 0$

$-14 = (-3)(5) + 1$ $q = -3$, $r = 1$.

Often we are interested only in r, not q.

Notation: If a, b, q, r, $b > 0$, $0 \leq r < b$ as in division algorithm, so that

$$a = qb + r$$

Then write $a \bmod b = r$

Def q is called the quotient & r the remainder

Observation:

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

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

Why?

$$a_1 = q_1 b + r_1 \quad , \quad a_2 = q_2 b + r_2$$

$$\Rightarrow \quad a_1 + a_2 = q_1 b + q_2 b + (r_1 + r_2)$$
$$= (q_1 + q_2) b + r_1 + r_2$$

Might not have $r_1 + r_2 < b$, but

by division algorithm $\exists\ q_3$ & $r < b$ $\quad r \geq 0$

with $$r_1 + r_2 = q_3 b + r \qquad (*)$$

so $$a_1 + a_2 = (q_1 + q_2 + q_3) b + r \qquad (**)$$

i.e. $$(a_1 + a_2) \bmod b = r = (r_1 + r_2) \bmod b$$

by (*) & (**)

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

check it!