BlankTemplate

Division Algorithm

$b \div m \rightarrow b = q m + r$ ← remainder ; $\boxed{0 \leq r < m}$

q ↑ quotient

Remainder : $r \geq 0$
Remainder is never negative

Ex] $33 \div 7$

mult 4 ← quotient

$$\begin{array}{r} 4 \\ 7\overline{)33} \\ -28 \\ \hline 5 \end{array}$$

5 ← remainder r

$\boxed{q = 4 \quad r = 5}$

$33 = \underset{q}{\underline{4}} \cdot 7 + \underset{r}{\underline{5}}$

Ex] $-33 \div 7$

$$\begin{array}{r} -5 \\ 7\overline{)-33} \\ \oplus\ -35 \\ \hline 2 \end{array}$$

$-5 \leftarrow q$

$2 \leftarrow r$

7 divides into -33 -5 times, $7(-5) = -35$, -35 is nearest integer <u>less</u> than -33 that 7 divides with a remainder of <u>2</u>

$\boxed{q = -5, \ r = 2}$

Computationally: $b \bmod m$ extracts the remainder of $b \div m$

Ex) $33 \bmod 7 \boxed{= 5}$

Ex) $-33 \bmod 7 \boxed{= 2}$

Find a Calculator method for doing: mod arithmetic

Generalization of Mod arithmetic

$a \equiv b \bmod m$

is congruent to

if $m \mid (a-b)$

Ex) $25 \equiv 11 \bmod 7$

since $7 \mid (25-11)$ or $7 \mid 14$

Another way to think of $\equiv$

$25 \equiv 11 \bmod 7$ since

$$\left.\begin{array}{l} 25 \bmod 7 = 4 \\ 11 \bmod 7 = 4 \end{array}\right\}$$

25 and 11 are $\equiv \bmod 7$ since they both give same remainder of 4 when divided by 7

$$\underbrace{25 \equiv 18 \equiv 11}_{\text{all of when divided by 7 give a remainder of 4}} \equiv 4 \mod 7$$

This defines a set called a congruence class!

$$\underbrace{\overline{4} = \{\ldots, -24, -17, -10, -3, 4, \overset{+7}{11}, \overset{+7}{18}, \overset{+7}{25}, \overset{+7}{32}, 39 \ldots\}}_{= \text{ class of numbers giving remainder of } 4}$$

Section 1

4b] Find the elements of congruence class $x \equiv \underline{7} \pmod{\underline{11}}$

$$\underbrace{\overline{7} = \{\ldots, -26, -15, -4, 7, \overset{+11}{18}, \overset{+11}{29}, 40, 51, \ldots\}}_{\text{set of integers that give a remainder of 7 when divided by 11}}$$

Euclidean Algorithm is designed to get the greatest common divisor, denoted as gcd(a, b), a and b are integers

Ex) $\boxed{\gcd(20, 30) = 10}$

Section 1

Ex) 2d.) Find the gcd of 3854682 and 1095939

Note! 3854682 > 1095939

start
$\boxed{3854682 \div 1095939 \approx 3.51}$

Never Shift Quotients

$3854682 \div 1095939$: $3854682 = \underline{3} \cdot 1095939 + \underline{566865}$ ← R1

$1095939 \div 566865 \rightarrow 1095939 = \underline{1} \cdot 566865 + \underline{529074}$ ← R2

$566865 \div 529074 \rightarrow 566865 = \underline{1} \cdot 529074 + \underline{37791}$ ← R3 ← last non-zero remainder is gcd

$529074 \div 37791 \rightarrow 529074 = \underline{14} \cdot 37791 + \underline{0}$

$\boxed{\text{stop remainder} = 0}$

$\boxed{\text{Hence, } \gcd(3854682, 1095939) = 37791}$

max # 3.

$$\begin{array}{r} 1095939 \,\overline{)\,3854682} \\ \underline{3287817} \\ 566865 \end{array}$$

$$\begin{array}{r} 1. \\ 566865 \,\overline{)\,1095939} \\ \underline{-\ 566865} \\ 529074 \end{array}$$

$$\begin{array}{r} 529074 \,\overline{)\,566865} \\ \underline{529074} \\ 37791 \end{array}$$

Fact: For GCD(a,b), there are integers u and v where
$au + bv = gcd(a,b)$

Ex Find u and v where $au + bv = gcd(a,b)$ when
$a = 3854682$ and $b = 1095939$

Run on Euclid Alg to find gcd(a,b) (Last Page)

Euclidean Algorithm Table

use 2x2 identity matrix to start u and v in table

Row	Q	R	U	V
-1	—	a = 3854682	$1 = u_{-1}$	$0 = v_{-1}$
0	—	b = 1095939	$0 = u_0$	$1 = v_0$
1	$q_1 = 3$	566865	$u_1 = 1$	$v_1 = -3$
2	$q_2 = 1$	529074	$u_2 = -1$	$v_2 = 4$
3	$q_3 = 1$	37791 gcd	$u_3 = 2$	$v_3 = -7$

3 rows in Euclid Alg to get to gcd

Final u and v come from gcd Row of table

u's: $u_{i+1} = u_{i-1} - q_{i+1} u_i$

Row 1 $u_1 = u_{-1} - q_1 u_0$
$u_1 = 1 - 3 \cdot 0 = 1$

Row2 $u_2 = u_0 - q_2 u_1$
$u_2 = 0 - 1 \cdot 1 = -1$

Row3 $u_3 = u_1 - q_3 u_2$
$u_3 = 1 - 1(-1) = 1 + 1 = 2$

v's: $v_{i+1} = v_{i-1} - q_{i+1} v_i$

Row 1: $v_1 = v_{-1} - q_1 v_0 = 0 - 3(1) = -3$

Row 2: $v_2 = v_0 - q_2 v_1 = 1 - (1)(-3) = 4$

Row 3: $v_3 = v_1 - q_3 v_2 = -3 - (1)(4) = -7$

$$\boxed{\text{Answer: } u = 2,\ v = -7}$$

Check: $au + bv = gcd(a,b)$
$(3854682)(2) + (1095939)(-7) \overset{?}{=} 37791$
✓ $37791 = 37791$

Page 6

Wednesday, July 17, 2019 4:25 PM

Extra Notes: over $\mathbb{Z}_4 \times \mathbb{Z}_7$

$$(3,5)\cdot(-2,4) = (3\cdot(-2),\ 5\cdot 4)$$

$$= (-6,\ 20)$$

$-6 \equiv 2 \bmod 4$, $20 \equiv 6 \bmod 7$

$$\boxed{= (2,6)}$$