3.3

11.5.04
Tutorial 6

P: Note that a is legal

$\Leftrightarrow \gcd(\check{a}, m) = 1$.

Suppose a, b are legal.

Then $\gcd(\underbrace{\check{a} \cdot \check{b}}_{\text{"}}, m) = 1$

$\gcd(\check{a} \cdot \check{b} - k \cdot m, m)$

$= \underbrace{\check{a}\check{b} \text{ rem } m}$

for some choice of k.

$\Rightarrow$ $a \cdot b$ is legal.

(Note: $a \cdot b \overset{\text{def}}{=} (\check{a} \cdot \check{b}) \text{ rem } m$.)

A: $\overbrace{(a \cdot b) \cdot c} = (\overbrace{a b} \cdot \check{c}) \text{ rem } m$

$= ((\check{a}\check{b} \overset{\text{"}a - k \cdot m\text{"}}{\text{rem } m}) \cdot \check{c}) \text{ rem } m$.

$= (\underbrace{(\check{a}\check{b}) \cdot \check{c}}) \text{ rem } m$

$= (\check{a} \overbrace{(b c)}) \text{ rem } m$

$\vdots$

$= a (b c)$.

11.05.04
Tutorial (2)

I:

	r		s	t	
x =	20		1	0	$20 = 1\cdot 20 + 0\cdot 9$
y =	9	2	0	1	$9 = 0\cdot 20 + 1\cdot 9$
	2	4	1	-2	
	1	2	-4	9	$1 = (-4)\cdot 20 + 9\cdot 9$
			9	-20	small $= s\cdot 20 + t\cdot 9$
	0				

Outcome: Last non-zero r is the gcd & the zero line gives us a simple test & we get a representation of the gcd as $= s\cdot x + t\cdot y$

gcd(x,y)

20
-9
"
$1 = 1\cdot 20 + (-1)\cdot 9$

$20 - 2\cdot 9 = (1\cdot 20 + 0\cdot 9)$
$= -2\,(0\cdot 20 + 1\cdot 9)$
$2 = 1\cdot 20 + (-2)\cdot 9$.

What we want is:

$a \cdot b = 1$ in $\mathbb{Z}_m^\times$

ie. $\check{a}\,\check{b} + k\cdot m = 1$
"
gcd($\check{a}$, m)

C: $\check{a}\cdot\check{b} = \ldots\ldots = \check{b}\cdot\check{a}$.