MAT315 Assignment 2 Rui Qiu #999292509

1. (ex 6.2(a))

Solution:

$\gcd(105,121)=1$

$121=105\times1+16$	$16=121-105$
$105=16\times6+9$	$9=105-(121-105)\times6=7\times105-6\times121$
$16=9\times1+7$	$7=16-9=121-105-7\times105+6\times121$
$9=7\times1+2$	$=7\times121-8\times105$
$7=2\times3+1$	$2=9-7=15\times105-13\times121$
$2=1\times2$	$1=7-2\times3$
	$=7\times121-8\times105-45\times105+39\times121$
	$=46\times121-53\times105$

So for $105x+121y=1$. $x=-53, y=46$ is a set of solution.

By Linear Equation Thm:
every other solution can be obtained by taking different k values into:

$$(-53+k\cdot121,\ 46-k\cdot105)$$
$$=(-53+121k,\ 46-105k) \quad \text{where } k\in\mathbb{Z}.$$

2. (ex. 6.4(c))

Solution: $155x+341y+385z=1$

$\gcd(341,385)=11$ by Euclidean algorithm

rewrite $155x+11(31y+35z)=1$

Let $31y+35z=u$

so $155x+11u=1$

$\gcd(155,11)=1$

Similarly using Euclidean algorithm, can get a set of solution for $155x+11u=1$, which is $x=1, u=-14$.

Now back to $31y'+35z'=1$

use Euclidean algorithm again, we can calculate that $y'=-9, z'=8$.

Now plug them back in the original equation.

$x=1,\ y=(-9)\times(-14)=126,\ z=8\times(-14)=-112$

Check $1\times155+341\times126+385\times(-112)=1$.

3. (ex 7.6)

Solution:

(a). By listing some numbers in $\mathbb{M}$:

$$\{1, 5, 9, 13, 17, 21, \underbrace{25}_{= 5\times 5}, 29, 33, 37, 41, 45, 49, \cdots\}$$

Note: The circled # is not M-prime.

So the first 6 M-primes are $\{5, 9, 13, 17, 21, 29\}$

(b). Know that: if $a \in \mathbb{M}$, $b \in \mathbb{M}$,

so $ab \in \mathbb{M}$

b/c $a \equiv b \equiv 1 \bmod 4 \equiv ab$

693 is such a number.

Check $693 = 21 \times 33 = 9 \times 77$

$3\times 7 \times 3 \times 11$

where $21, 33, 9, 77$ are all M-primes.

4. (ex. 8.5(c))

Solution: $21x \equiv 14 \bmod 91$

$\gcd(21, 91) = 7$

$91 = 21 \times 4 + 7$

$21 = 7 \times 3$

since $7 \mid 14$, by Linear Congruence Thm,

there are exactly 7 incongruent solutions to this equation.

$21u - 91v = 7$ has 7 solutions. $(*)$

$3u - 13v = 1$

we can locate the first set of solution $(u_0, v_0) = (-4, -1)$ fast.

So the other solutions to $(*)$ is in form of:

$$(-4 + (-13)k, -1 - k(3)) = (-4 - 13k, -1 - 3k)$$

so $x_0 = \frac{c u_0}{g} = \frac{14\times(-4)}{7} = -8$

$x \equiv x_0 + k\cdot\frac{91}{7} \mod 91 = -8 + 13k \mod 91$

Plug in different k, we can get:

$x = 5, 18, 31, 44, 57, 70, 83.$

5. (ex. 9.1(c))

Solution: $x^{39} \equiv 3 \mod 13$

by Fermat's little Thm:

$x^{12} \equiv 1 \mod 13$

rewrite: $x^{39} \equiv x^{36+3} \equiv (x^{12})^3 x^3 \equiv x^3 \equiv 3 \mod 13$

But, by listing all of x mod 13 & x^3 mod 13:

x mod 13	0	1	2	3	4	5	6	7	8	9	10	11	12
x^3 mod 13	0	1	8	1	12	8	8	5	5	1	12	5	12

And obviously, there's no integer solutions to this equation.

6. (ex 9.2).

Solution:

(a) Note: p is prime number.

p	$(p-1)!$	$(p-1)!$ mod p
2	1	1 mod 2
3	2	2 mod 3
5	24	4 mod 5
7	720	6 mod 7
11	3628800	10 mod 11
13	⋮	⋮
17	⋮	⋮
19		

Conjecture: for p prime, the value of $(p-1)!$ mod p is $(p-1)$ mod p.

(2). Actually it's Wilson's Thm.

Proof:

Since p is prime, all integers smaller than p is relatively prime to it.

For each integer s, there exists $t \in \mathbb{Z}$ such that $s, t < p$ and $s \cdot t \equiv 1 \mod p$.

and $s = t$ iff $s = 1$ or $p-1$.

hence $2 \cdot 3 \cdots (p-2) \equiv 1 \mod p$.

Then $(p-1)! \equiv (p-1) \mod p$ as desired.

$\blacksquare$