Solution, Weston's Practice Midterm 2

Problem 1: (a) $17x_i + 11y_i = r_i$

x_i	y_i	r_i	q_i
1	0	17	
0	1	11	
1	-1	6	1
-1	2	5	1
2	-3	1	1

$2 \cdot (17) + (-3)\,11 = 1$

So $\overline{11}^{-1} = -\overline{3} = \overline{14}$ in $\mathbb{Z}_{17}$.

(b) $\overline{7} \cdot \overline{11}^{-1} = (-\overline{3}) \cdot \overline{7} = -\overline{21} = \overline{13}$ in $\mathbb{Z}_{17}$.

Problem 2: 101 is a prime.

So $\bar{a}^{100} = \overline{1}$ in $\mathbb{Z}_{101}$, if $\bar{a} \neq \bar{0}$.

So $\overline{31}^{1209} = \overline{31}^{1200+9} = \underbrace{\left(\overline{31}^{100}\right)^{12}}_{\overline{1}} + \overline{31}^{9} =$

$= \overline{31}^{-9} = \overline{31}^{8} \cdot \overline{31}$

$\overline{31}^{2} = \overline{961} = \overline{52}$ in $\mathbb{Z}_{101}$

$\overline{31}^{4} = \overline{52}^{2} = \overline{2704} = -\overline{23}$

$\overline{2727} - \overline{23}$

$\overline{31}^{8} = -\overline{23}^{2} = \overline{529} = \overline{24}$

$\overline{505} + \overline{24}$

So $\overline{31}^{9} = \overline{24} \cdot \overline{31} = \overline{744} = \overline{37}$

$\overline{707} + \overline{37}$

So $\overline{31}^{1209} = \overline{37}$ in $\mathbb{Z}_{101}$.

$11 \cdot 17 = n$

Problem 3: RSA code with $n = 187$ and $e = 23$.

The decoding exponent d should satisfy $ed \equiv 1 \pmod{\varphi(n)}$.

$\varphi(n) = \varphi(11 \cdot 17) = \varphi(11)\,\varphi(17) = 10 \cdot 16 = 160$.

$160 x_i + 23 y_i = r_i$

x_i	y_i	r_i	q_i
1	0	160	
0	1	23	
1	−6	22	6
−1	7	1	1

$(-1) \cdot 160 + 7 \cdot 23 = 1$

So $d = 7$

Encripted message 144

$144^7 = 144^{4+2+1} = 144^4 \cdot 144^2 \cdot 144 \equiv 1601568$

$144^4 \equiv 67$, $144^2 \equiv 111$, $67 \cdot 111 \equiv 166 \pmod{187}$

$\equiv \boxed{100} \pmod{187}$.

So, the decoded message is 100.

Problem 4: How many zeros does $62!$ end in?

There are $\frac{60}{5} = 12$ integers k in the range $1 \le k \le 62$, which are divisible by 5.

Two of them are divisible by $25 = 5^2$, namely 25 and 50. So $5^{14} \mid 62!$, and $5^{15} \nmid 62!$.

There are $\frac{62}{2} = 31$ integers k in the range $1 \le k \le 62$, which are divisible by 2.

Hence, $2^{14} \mid 62!$. Thus, $10^{14} \mid 62!$, but $10^{15} \nmid 62!$.

So $62!$ ends with 14 zeroes.

Problem 5:

(1) $8X \equiv 7 \pmod{11}$

$\bar{X} = \bar{8}^{-1} \cdot \bar{7}$

$11x_i + 8y_i = r_i$ $\quad 11 \cdot 3 - 8 \cdot 4 = 1$

1	0	11
0	1	8
1	-1	3
-2	3	2
3	-4	1

So $\bar{8}^{-1} = \bar{4}$ in $\mathbb{Z}_{11}$

$\bar{X} = \bar{4} \cdot \bar{7} = \overline{28} = \bar{6}$ in $\mathbb{Z}_{11}$

$X = \{6 + 11k : k \in \mathbb{Z}\}$.

(2) $36X = 18 \pmod{60}$.

$\gcd(36, 60) = 2^2 \cdot 3 = 12 \nmid 18$

$36 = 2^2 \cdot 3^2$, $\quad 60 = 2^2 \cdot 3 \cdot 5$

Hence, a solution does not exist,

since a soln to $36X + 60y = 18$ exists,

if and only if $\gcd(36, 60) \mid 18$.

(3) $5X \equiv 15 \pmod{25}$

One solution is $x_0 = 3$.

$5x \equiv 15 \pmod{25}$

$\Leftrightarrow$

$\exists y \in \mathbb{Z}, \quad 5x + 25y = 15$

$\Leftrightarrow$

$\exists y \in \mathbb{Z}, \quad x + 5y = 3$

The general soln of $\uparrow$ is

$(x, y) = (3, 0) + k(-5, 1), \quad k \in \mathbb{Z}.$

So, $\exists y \in \mathbb{Z}, \; x + 5y = 3$

$\Leftrightarrow$

$\{x = 3 - 5k, \quad k \in \mathbb{Z}\}$

Problem 6:

(a) $\frac{1}{5} \in \mathbb{Z}_{13}$. In our notation this means compute 5^{-1}. There is a unique inverse, which is -5:

$$\bar{5}(-\bar{5}) = -\bar{25} = \bar{1} \text{ in } \mathbb{Z}_{13}$$

(b) $\frac{3}{7} \in \mathbb{Z}_{14}$. In our notation this means find all solutions x of $\bar{7}x = \bar{3}$ (*) in $\mathbb{Z}_{14}$.

Now $\bar{3}^{-1} = \bar{5}$ in $\mathbb{Z}_{14}$, so if x is a solution then it is also a sol'n of $\underbrace{\bar{5}\cdot\bar{7}}_{\bar{35}=\bar{7}}\bar{x} = \bar{1}$

But $\gcd(7,14) \neq 1$, so $\bar{7}$ is not invertible in $\mathbb{Z}_{14}$. Thus, a solution for (*) does not exist.

(c) $\sqrt{5} \in \mathbb{Z}_{11}$. In our notation this mean find all solutions of $x^2 = \bar{5}$ in $\mathbb{Z}_{11}$. Now $\bar{5} = \bar{16} = \bar{4}^2$ in $\mathbb{Z}_{11}$. So $x^2 - \bar{5} = (x-\bar{4})(x+\bar{4})$. If $x \in \mathbb{Z}_{11}$ is a root, then either it is a root of $(x-\bar{4})$ or a root of $(x+\bar{4})$, since 11 is a prime. So $x = \bar{4}$ or $x = -\bar{4}$.

(d) $\sqrt{-1} \in \mathbb{Z}_{11}$. In our notation this means find all solutions of $x^2 = -1$ in $\mathbb{Z}_{11}$.

A solution does not exists, for example by the table in $\mathbb{Z}_{11}$

x	$\bar{1}$	---
x^2	$\bar{1}$	---

(e) $\sqrt[3]{\bar{2}} \in \mathbb{Z}_5$. This means find all sol'n of $x^3 = \bar{2}$ in $\mathbb{Z}_5$ in our notation.

x	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
x^3	$\bar{0}$	$\bar{1}$	$\bar{3}$	$\bar{2}$	$\bar{4}$

There exists a unique sol'n, $x = \bar{3}$, by the table.