Western Practice Final

2) All positive integers n such that

$12 \mid n$ and $n \mid 816$

$12 = 2^2 \cdot 3$

$816 = 16 \cdot 51 = 2^4 \cdot 3 \cdot 17$

$$n = 2^{e_1} \cdot 3^{e_2} \cdot 17^{e_3}$$

$2 \leq e_1 \leq 4$ $\quad \boxed{e_1 \in \{2, 3, 4\}}$

$\boxed{e_2 = 1}$

$0 \leq e_3 \leq 1$ $\quad \boxed{e_3 \in \{0, 1\}}$

So, there are 6 such positive integers

3) $11x + 17y = 305, \quad x, y \in \mathbb{Z}^+$

$17 y_i + 11 x_i = r_i$

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

$2 \cdot 17 - 3 \cdot 11 = 1$

$x_0 = \underbrace{(-3) \cdot 305}_{-915}, \quad y_0 = \underbrace{2 \cdot 305}_{610}$

The general sol'n:

$(x, y) = (x_0 + 17k, y_0 - 11k) =$

$= (17k - 915, 610 - 11k)$

$17K - 915 > 0$

$K > 915/17 = 53,82\ldots$

$610 - 11K > 0$

$K < \frac{610}{11} = 55,\overline{45}$

$K \in \{54, 55\}$

4) $31^{1209} \pmod{101} = (31^{100})^{12} \cdot 31^{9}$

m p c

$31^2 = 961 \equiv 52$

$31^4 = 52^2 = 2704 \equiv -23$

$31^8 = (-23)^2 \equiv 23^2 = 24$

$31^9 \equiv 24 \cdot 31 = 744 = \boxed{37}$

5) Solve

$$(*)\quad \begin{cases} t \equiv 2 \pmod{10} \\ t \equiv 7 \pmod{11} \end{cases}$$

$\gcd(10,11)=1$

Solve $10x + 11y = 7-2 = 5$ (+)

$(x_0, y_0) = (-5, 5)$ is a sol'n.

Then $t = \underbrace{10x+2}_{\equiv 2 \pmod{10}} = \underbrace{7-11y}_{\equiv 7 \pmod{11}}$

Now $t_0 = 10x_0 + 2 = -48$ is a sol'n for (*), and the general sol'n is $t = t_0 + K(10\cdot 11)$ by the Chinese Remainder Theorem. $\mathbb{Z}$

6) How many roots does $f(x) = x^8 - 1$ has in $\mathbb{Z}_{91}$?

Note: $91 = 7 \cdot 13$

In $\mathbb{Z}_7$ ~~if $\bar{x} \neq \bar{0}$~~, then $\bar{x}^8 = \bar{x}^2$, by Fermat's Little Theorem, Now $\bar{1}, -\bar{1}$ are the two soln of $x^2 - \bar{1} = 0$, by Prop 10.2.2, page 434,

In $\mathbb{Z}_{13}$, if $\bar{x}^8 = \bar{1}$, then $\bar{x}^{\gcd(8,13-1)} = \bar{x}^4 = \bar{1}$, because $\text{ord}(\bar{x}) \mid 8$ and $\text{ord}(\bar{x}) \mid 13-1 = 12$,

Furthermore, $\bar{x}^4 = \bar{1}$ has 4 soln's by Prop 10.2.2, since $4 \mid (13-1)$.

So, $f(x) = x^8 - 1$ has $4 \cdot 2 = 8$ soln in $\mathbb{Z}_{91}$, by the Chinese Remender Theorem

$2 \cdot 99 = 2 \cdot 11 \cdot 9$

8) $\left(\frac{198}{223}\right) = \left(\frac{2}{223}\right)\left(\frac{11}{223}\right)\left(\frac{9}{223}\right)$

$223 \equiv -1 \pmod 8$, so $\left(\frac{2}{223}\right) = 1$,

by The quadratic character for 2 Theorem 11.4.3,

$$\left(\frac{11}{223}\right) = -\left(\frac{223}{11}\right) = -\left(\frac{3}{11}\right) = \left(\frac{11}{3}\right) = \left(\frac{2}{3}\right) = \underline{-1}$$

$11 \equiv 3 \pmod 4$

$223 \equiv 3 \pmod 4$

$\left(\frac{9}{223}\right) = 1$, since by the Multiplicativity of the Legendre Symbol,

$= \left(\frac{3}{223}\right)^2$

So $\left(\frac{198}{223}\right) = (-1)(-1)(1) = \underline{1}$

Problem 9: $n = 187$

$= 11 \cdot 17$

$e = 23$

$\varphi(187) = (11-1)(17-1) = 160$

$\gcd(160, 23) = 1$, since 23 is a prime and $23 \nmid 160$

Decoding exponent: d

$\bar{d} = \bar{e}^{-1}$ in $\mathbb{Z}_{160}$

$160x + 23d = 1$

x_i	d_i	r_i	q_i
1	0	160	
0	1	23	
1	-6	22	6
-1	7	1	1

$d = 7$

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

Decode 144

$144^7 = ?$

$144^2 \equiv 20736 \equiv 166 \pmod{187}$

$144^4 \equiv 166^2 = 27556 \equiv 67 \pmod{187}$

$144^7 \equiv 144^4 \cdot 144^2 \cdot 144 \equiv 67 \cdot 166 \cdot 144 \equiv$

$\equiv 100 \pmod{187}$

Problem 11: Find the general sol'n of $17x + 31y = 3$ (*)

$\gcd(17, 31) = 1$

$31 y_i + 17 x_i = r_i$

y_i	x_i	r_i
1	0	31
0	1	17
1	−1	14
−1	2	3
5	−9	2
−6	11	1

gcd

$-6(31) + 17 \cdot 11 = 1$

One particular sol'n of (*) is

$(x_0, y_0) = 3(11, -6) = (33, -18)$.

The general sol'n is

$(x, y) = (33 - 31k, -18 + 17k), \quad k \in \mathbb{Z}$

Problem 12; $n \in \mathbb{N}$, $\bar{a} \in \mathbb{Z}_n$, $e := \operatorname{ord}(\bar{a})$

Then $\operatorname{ord}(\bar{a}^2) = \dfrac{\operatorname{ord}(\bar{a})}{\gcd(2, \operatorname{ord}(\bar{a}))} =$

↑ Lemma 10, 1, 6 page 423

$$= \begin{cases} \operatorname{ord}(\bar{a}) & \text{if } \operatorname{ord}(\bar{a}) \text{ is odd} \\ \dfrac{\operatorname{ord}(\bar{a})}{2} & \text{" " " even,} \end{cases}$$

Problem 13:

(a) $t \equiv 4 \pmod 7$

$t \equiv 10 \pmod{13}$,

$\gcd(7, 13) = 1$, so we can use the Chinese Remainder Theorem.

Solve $7x + 13y = 10 - 4 = 6$

(the Diophantine eq)

If (x, y) is a solution, then

then $t = 7x + 4 = 10 - 13y$ solves the simultaneous Diophantine eq.

$(x, y) = (12, -6)$ is a soln,

so $\boxed{t = 7 \cdot 12 + 4 = 88}$ is a soln.

(b) $\begin{cases} (1)\ x \equiv 11 \pmod{12} \\ (2)\ x \equiv 5 \pmod{14} \\ (3)\ x \equiv 19 \pmod{21} \end{cases}$

$(1) \Rightarrow x \equiv 11 \equiv 2 \pmod 3$

$(3) \Rightarrow x \equiv 19 \equiv 1 \pmod 3$

Hence, a solution does NOT exist.