(c) **Thm** If a is odd, then $12 \mid a^2+(a+2)^2+(a+4)^2+1$.

pf Write $a = 2k+1$, for some $k \in \mathbb{Z}$

So $a^2+(a+2)^2+(a+4)^2+1$

$= 4k^2+4k+1 + (2k+3)^2 + (2k+5)^2+1$

$= 4k^2+4k+1 + 4k^2+12k+9 + 4k^2+20k+25+1$

$= 12k^2+36k+36.$

Since $12 \mid 12k^2$, $12 \mid 36k$ and $12 \mid 36$,

we have $12 \mid 12k^2+36k+36$ //

(d) **Thm** If $n = a^2+b^2$, then $n \neq 4m+3$ for any $m \in \mathbb{Z}$.

pf Note that $0^2 \equiv 0 \pmod 4$ $1^2 \equiv 1 \pmod 4$

$2^2 \equiv 0 \pmod 4$ $3^2 \equiv 1 \pmod 4$.

So $x^2 \equiv 0$ or $1 \pmod 4$

Thus, $a^2+b^2 \equiv \begin{cases} 0 & \text{if } a, b \equiv 0 \text{ or } 2 \pmod 4 \\ 1 & \text{if } a \equiv 0 \text{ or } 2 \pmod 4 \text{ and } b \equiv 1 \text{ or } 3 \pmod 4 \text{ (or vice versa)} \\ 2 & \text{if } a, b \equiv 1 \text{ or } 3 \pmod 4. \end{cases}$

Therefore, $a^2+b^2 \equiv 3 \pmod 4$ is impossible. //

(e) **Thm** If m and n have no common prime factor then $m+n$ and m have no common prime factor.

pf We prove the contrapositive.

Assum $m+n$ and m have a common prim factor, say p. That is, p is prime and $p \mid m+n$ and $p \mid m$.

Then $p \mid (m+n-m) = n$. Hence, $p \mid m$ and $p \mid n$.

So m and n have a common prim factor //

(f)
$366 = 1 \cdot 234 + 132$
$234 = 1 \cdot 132 + 102$
$132 = 1 \cdot 102 + 30$
$102 = 3 \cdot 30 + 12$
$30 = 2 \cdot 12 + 6$
$12 = 2 \cdot 6$

$\gcd(366, 234) = 6$

(g) By back substitution,

$$\begin{aligned}
6 &= 30 - 2\cdot 12 \\
&= (132 - 102) - 2(102 - 3\cdot 30) \\
&= 132 - 3\cdot 102 + 6\cdot 30 \\
&= (366 - 234) - 3(234 - 132) + 6(132 - 102) \\
&= 366 - 4\cdot 234 + 9\cdot 132 - 6\cdot 102 \\
&= 366 - 4\cdot 234 + 9\cdot(366 - 234) - 6(234 - 132) \\
&= 10\cdot 366 - 19\cdot 234 + 6\cdot 132 \\
&= 10\cdot 366 - 19\cdot 234 + 6\cdot(366 - 234) \\
&= 16\cdot 366 - 25\cdot 234
\end{aligned}$$

Thus, $234x + 366y = 6$ has the soln $x = -25,\ y = 16$.

To get a soln for $234x + 366y = 126$ we multiply by 21.

So one soln is $\boxed{x = -525,\ y = 336}$

If $x = -525 + x_0$, $y = 336 + y_0$ such that then

$$\begin{aligned}
&234(-525 + x_0) + 366(336 + y_0) = 6 \\
\text{then}\quad &234x_0 + 366y_0 = 0 \\
\Rightarrow\ &366y_0 = -234x_0 \\
\Rightarrow\ &61y_0 = -39x_0 \\
\Rightarrow\ &x_0 = 61k \text{ for some } k \in \mathbb{Z} \\
&y_0 = -39k.
\end{aligned}$$

Thus, $\boxed{\begin{aligned} x &= -525 + 61k \\ y &= 336 - 39k \end{aligned} \text{ for } k \in \mathbb{Z}}$.

6 (a) $\sum_{k=0}^{11} \binom{11}{k} 7^k (-8)^{11-k} = (7-8)^{11} = (-1)^{11} = \boxed{-1}$

$\sum_{k=0}^{n} \binom{n}{k} w^k (w+1)^{n-k} = (w-(w+1))^n = \boxed{(-1)^n}$

(b) **Thm** If $\binom{n-2}{k}$ AND $\binom{n-2}{k-2}$ are odd, then $\binom{n}{k}$ is even

pf) From Exam 2, $\binom{n}{k} = \binom{n-2}{k} + 2\binom{n-2}{k-1} + \binom{n-2}{k-2}$.

Since $\binom{n-2}{k}$ & $\binom{n-2}{k-2}$ are odd,

$\binom{n-2}{k} = 2r+1$ and $\binom{n-2}{k-2} = 2t+1$

for some $r, t \in \mathbb{Z}$

Thus, $\binom{n}{k} = 2r+1 + 2\binom{n-2}{k-1} + 2t+1$

$= 2\left(r + \binom{n-2}{k-1} + t + 1\right)$

is even //

(c) **Thm** $m \mid (m+1)^k - 1$.

pf)

By the binomial theorem,

$(m+1)^k = \sum_{\ell=0}^{k} \binom{k}{\ell} m^\ell$

$\Rightarrow (m+1)^k - 1 = \sum_{\ell=1}^{k} \binom{k}{\ell} m^\ell$

Thus, $(m+1)^k - 1 = m\left[\sum_{\ell=1}^{k} \binom{k}{\ell} m^{\ell-1}\right]$

which is always an integer because $\ell \geq 1$.

Therefore, m divides $(m+1)^k - 1$. //

7(a) **Thm** $7 \mid 6^n - 1$ iff n is odd.

pf Note: $6 \equiv -1 \pmod 7$

So $6^n \equiv (-1)^n \equiv \begin{cases} 1 \pmod 7, & \text{if } n \text{ is even} \\ -1 \pmod 7, & \text{if } n \text{ is odd.} \end{cases}$

Thus,

$7 \mid 6^n - 1 \iff 6^n - 1 \equiv 0 \pmod 7$

$\iff 6^n \equiv 1 \pmod 7$

$\iff (-1)^n \equiv 1 \pmod 7$

$\iff n$ is odd. //

(b) $5x \equiv 3 \pmod{18}$

we know that $5^{-1} \pmod{18}$ exists because $\gcd(5, 18) = 1$.

Now we experiment (Note that the inverse, 5^{-1}, will also be relatively prime to 8)

$5 \cdot 1 \equiv 5 \pmod{18}$

$5 \cdot 5 \equiv 7$ "

$5 \cdot 7 \equiv 17$ " "

$5 \cdot 11 \equiv 1$ "

Thus, $5^{-1} \equiv 11 \pmod{18}$

Hence,

$11 \cdot 5x \equiv 11 \cdot 3 \pmod{18}$

$x \equiv 33 \pmod{18}$

$x \equiv 15 \equiv -3 \pmod{18}$

(c) $182000000147743273^4 \equiv 3^4 \pmod{10}$

$\equiv 81 \equiv 1 \pmod{10}$

(d) **Thm** If $bc \equiv bd \pmod p$, p a prime, and $p \nmid b$, then $c \equiv d \pmod p$.

pf Since $bc \equiv bd \pmod p$, by def'n,

$p \mid bc - bd = b(c-d)$.

Since $p \nmid b$ and p is a prime, $\gcd(b, p) = 1$.

Thus, $p \mid c - d \Rightarrow c \equiv d \pmod p$ //

(e) **Thm** Let $n \in \mathbb{N}$. $3 \mid n \iff$ 3 divides the sum of the base 10 digits of n.

pf) Write $n = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \cdots + a_r 10^r$ with $0 \le a_i < 10$ integers for $i = 0, 1, 2, \ldots, r$.
(This is the base 10 representation of n.)
Since $10 \equiv 1 \pmod 3$, we have
$10^i \equiv 1^i \equiv 1 \pmod 3$ for $i \ge 1$.

Thus,
$n \equiv \underbrace{a_0 + a_1 + a_2 + \cdots + a_r}_{\text{sum of the digits of } n.} \pmod 3$

Hence,
$3 \mid n \iff n \equiv 0 \pmod 3$
$\iff a_0 + a_1 + a_2 + \cdots + a_r \equiv 0 \pmod 3$
$\iff$ 3 divides the sum of the base 10 digits of n. //

(f) **Thm** If $ab \equiv 0 \pmod n$ and $b \not\equiv 0 \pmod n$ then $a \equiv 0 \pmod n$ or $\gcd(b, n) > 1$.

pf) Let $ab \equiv 0 \pmod n$ and $b \not\equiv 0 \pmod n$.
Certainly, $a \equiv 0 \pmod n$ is one possibility.
Assume $a \not\equiv 0 \pmod n$.
We will show that $\gcd(b, n) > 1$ must be true.
Since $ab \equiv 0 \pmod n$, $n \mid ab$.
Since $b \not\equiv 0 \pmod n$ and $a \not\equiv 0 \pmod n$,
$n \nmid b$ and $n \nmid a$.
If $\gcd(b, n) = 1$, then, by a result from class, n would have to divide a.
Thus, $\gcd(b, n) > 1$.
So we have shown that either
$a \equiv 0 \pmod n$ or $\gcd(b, n) > 1$
must be true. //

(g) **Thm** If $\gcd(a^2+a+1, n) = 1$ and $a^3 \equiv 1 \pmod{n}$, then $a \equiv 1 \pmod{n}$.

pf Since $a^3 \equiv 1 \pmod{n}$, by def'n,
$n \mid a^3 - 1$.
Observe $a^3 - 1 = (a-1)(a^2+a+1)$.
Thus, since $\gcd(a^2+a+1, n) = 1$, we know
$n \mid a-1$.
Hence, $a \equiv 1 \pmod{n}$ //

Example ① $n = 21$, $a = 4$ so $a^2+a+1 = 21$
$\gcd(a^2+a+1, n) = 21 > 1$
$a^3 = 4^3 \equiv 1 \pmod{21}$
$a \not\equiv 1 \pmod{21}$

② $n = 9$, $a = 7$ so $a^2+a+1 = 57$
$\gcd(a^2+a+1, n) = 3 > 1$
$a^3 = 7^3 \equiv 1 \pmod{9}$
$a \not\equiv 1 \pmod{9}$.