7. Examples.

1) What are the last digits in the decimal expansion of 3^{400}?

<u>Soln</u>: $3^{20} \equiv 1 \pmod{25}$ by $\underbrace{\text{Fermat}}^{\text{-Euler}}$ theorem.
Also, $3^2 \equiv 1 \pmod 4$. So, $3^{20} \equiv 1 \pmod{100}$.
So, $3^{400} = 3^{20} \cdot 3^{20} \cdots 3^{20}$ (20 times) $\equiv 1 \pmod{100}$
and the last 2 digits are ...01.

2) Show that (i) $\binom{p^n}{k} \equiv 0 \pmod p$ for $0 < k < p^n$;
(ii) $\binom{p^n - 1}{k} \equiv (-1)^k \pmod p$ for $0 < k < (p^n - 1)$

<u>Hint</u>: Use the identities

$$\binom{p^n}{k} = \binom{p^n-1}{k-1} \frac{p^n}{k}$$

$$\binom{p^n-1}{k} = \binom{p^n}{k} - \binom{p^n-1}{k-1}$$

3.11

3) a) If p is an odd prime, then (i) $x^2 \equiv 1 \pmod{p}$ if and only if $x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$.

(ii) $x^2 \equiv 1 \pmod{p^n}$ has only 2 solutions; $x \equiv 1 \pmod{p^n}$ and $x \equiv -1 \pmod{p^n}$

b) $x^2 \equiv 1 \pmod{2^n}$ has only one solution if $n = 1$; two solutions if $n = 2$; and precisely four solutions $\sim 1, 2^{n-1}+1, 2^{n-1}-1, -1$ if $n \geq 3$.

4) Determine if the system of congruences 7.3

$x \equiv 8 \pmod{15}$, $x \equiv 3 \pmod{10}$, $x \equiv 5 \pmod{84}$

has a common solution. If so, find all integers which satisfy this system simultaneously.

Sol: First recall:

Lemma. (i) $ax \equiv ay \pmod{m} \Leftrightarrow x \equiv y \bmod \left(\frac{m}{(a,m)}\right)$

(ii) $ax \equiv ay \pmod{m}$, $(a,m)=1$
$\Rightarrow x \equiv y \pmod{m}$

(iii) $x \equiv y \pmod{m_i}$, $i=1,\dots,r$ if, and only if, $x \equiv y \pmod{[m_1,\dots,m_r]}$
where $[m_1,\dots,m_r]$ is the LCM of $m_1,\dots,m_r$.

We use (iii). Pf: Exc. $\square$

By (iii), $x \equiv 8 \pmod{15}$ is equivalent to
$x \equiv 8 \pmod{3}$ and $x \equiv 8 \pmod{5}$.

7.4

$x \equiv 3 \pmod{10}$ is equivalent to

$x \equiv 3 \pmod 2$ and $x \equiv 3 \pmod 5$; and

$x \equiv 5 \pmod{84}$ is equivalent to

$x \equiv 5 \pmod 4$, $x \equiv 5 \pmod 3$ and

$x \equiv 5 \pmod 7$.

So, we need to find all integers x which satisfy the congruences

$$\left.\begin{aligned} x &\equiv 2 \pmod 3\\ x &\equiv 3 \pmod 5\\ x &\equiv 1 \pmod 2\\ x &\equiv 1 \pmod 4\\ x &\equiv 5 \pmod 7 \end{aligned}\right\}$$

Of these, $x \equiv 1 \pmod 2$ can be dropped, because $x \equiv 1 \pmod 4$ implies it. So, we need to find all $x \in \mathbb{Z}$ such that

$$\begin{aligned} x &\equiv 1 \pmod 4\\ x &\equiv 2 \pmod 3\\ x &\equiv 3 \pmod 5\\ x &\equiv 5 \pmod 7 \end{aligned}$$

By Chinese Rem. thm any solution is n is such that

$n \equiv 173 \pmod{420}$.

5) <u>Solve</u>: $17x \equiv 9 \pmod{276}$ 7:5

<u>Soln</u>: Since $276 = 3\cdot 4\cdot 23$, $17x \equiv 9 \pmod{276}$ is equivalent to

$$\left.\begin{array}{l} 17x \equiv 9 \pmod{3} \\ 17x \equiv 9 \pmod{4} \\ 17x \equiv 9 \pmod{23} \end{array}\right\} \text{i.e., to} \left\{\begin{array}{l} x \equiv 0 \pmod{3} \\ x \equiv 1 \pmod{4} \\ 17x \equiv 9 \pmod{23} \end{array}\right.$$

$x \equiv 0 \pmod{3} \Rightarrow x = 3k$ for <u>any</u> $k \in \mathbb{Z}$.

So $x \equiv 1 \pmod{4} \Rightarrow x = 3k \equiv 1 \pmod{4}$ — (*)

Multiplying (*) by 3 (<u>Note</u>: In $\mathbb{Z}_4^*$, $3^2 \equiv 1$) we have $k = 3 \pmod{4}$, so $k = 3 + 4j$ for <u>any</u> $j \in \mathbb{Z}$. Then $x = 3k = 3(3+4j) = 9 + 12j$ for <u>any</u> choice of $j \in \mathbb{Z}$. Now,

$$\begin{aligned} 17x \equiv 9 \pmod{23} \Rightarrow 17(9+12j) &\equiv 9 \pmod{23} \\ 204j &= -144 \pmod{23} \\ \text{or} \quad 3j &\equiv 6 \pmod{23} \\ \text{or} \quad j &\equiv 2 \pmod{6} \end{aligned}$$

So, $j = 2 + 23l$ for any $l \in \mathbb{Z}$

So, $x = 9 + 12j = 9 + 12(2 + 23l) = 33 + 276j$

So, all integer x, $x \equiv 33 \pmod{276}$ are solutions.

Exc. (Bramhaguptas, 7th century A.D.) When eggs from a basket are removed 2, 3, 4, 5, 6 at a time, their remain, respectively, 1, 2, 3, 4, 5 eggs. When they are taken out 7 at a time, no eggs are left. Find the smallest number of eggs that could have been in the basket. What is the next possible larger number of eggs in the basket?

7. Diaphontine equations

These are equation defined only in terms of integers and their solutions are also sought in terms of integers. We see some linear equations over integers.

<u>Ex.</u> Find the general form of the solutions of $5x + 22y = 18$ in integers, if it exists.

<u>Sol^n</u>: Since x has to be an integer, $x = (18-22y)/5$ must be an integer. Now,

$$x = \frac{18-22y}{5} = 3 - 4y + \frac{3-2y}{5}, \text{ so } \frac{3-2y}{5} =: z$$

also must be an integer. So

$$z = \frac{3-2y}{5} \quad \text{or} \quad 2y + 5z = 3.$$ As above

$$y = \frac{3-5z}{2} = 1 - 2z + \frac{1-z}{2}.$$ So, we need

$\frac{1-z}{2} =: t$ must be an integer. Then, $z = 1-2t$ is an integer. So,

$$y = \frac{3-5z}{2} = \frac{3-5(1-2t)}{2} = -1+5t,$$

and $$x = \frac{18-22y}{5} = \frac{18-22(-1+5t)}{5} = 8-22t$$

are solutions for all integers t. $\square$

Note 1: Geometrically, the above says that the line in $\mathbb{R}^2$ with equation $5x+22y=18$ intersects the lattice $\mathbb{Z}^2$ in $\mathbb{R}^2$ at points $\{(8-22t, -1+5t) : t \in \mathbb{Z}\}$.

Note 2: We prove the following

Theorem (i) A necessary and sufficient condition for the equation $ax+by=c$, — (1) $(a, b, c \in \mathbb{Z})$ to have a solution is that $d \mid c$, where $d = \gcd(a, b)$.

(ii) If there is one solution (x_0, y_0), then there are infinitely many solutions and they are exactly, $x = x_0 + \frac{b}{d}t$, $y = y_0 - \frac{a}{d}t$.

Note: $(a', b') = 1$

Proof: (i) If a integer solution x_0, y_0 exists for (1), since $d | a$ and $d | b$, then $d | ax + by = c$.
On the other hand, if $d | c$, there exist x_0', y_0' (in integers) such that $x = x_0'$, $y = y_0'$ is ~~are~~ a solution to $a'x + b'y = 1$ —(2), where $a' = a/d$, $b' = b/d$. ~~and~~ If $c' = c/d$, then $x_0 = c'x_0'$, $y_0 = c'y_0'$ is a solution to the equation $a'x + b'y = c'$ —(3)

So, x_0, y_0 will be a solution to (1) also.
(Note that every solution (2) is also a solution of (1).)

~~7.(1)~~

(ii) Now suppose (x_0, y_0) is a solution to (2). and (x_1, y_1) is any other solution of (2). Then, $a' x_0 + b' y_0 = c'$, $a' x_1 + b' y_1 = c'$. So,

$a'(x_0 - x_1) = b'(y_1 - y_0)$. Since $a' \mid b'(y_1 - y_0)$ and $(a', b') = 1$, $a' \mid y_1 - y_0$. Similarly, $b' \mid x_1 - x_0$. Since $\dfrac{a'}{b'} = \dfrac{y_1 - y_0}{x_0 - x_1}$, it follows that there is an integer t such that: $x_0 - x_1 = b't$ and $y_1 - y_0 = a't$; so, $x_1 = x_0 - b't$ and $y_1 = y_0 + a't$.

Conversely, (x_1, y_1) is a solution of (2) and so a solution of (1). □

7.1. If $ax + by = c$ — (1), $a, b, c \in \mathbb{Z}$, has a solution (i.e., $d = (a, b) \mid c$), we need to find <u>one</u> solutions (x_0, y_0), sometimes a positive solution (i.e., x_0, y_0 positive integers).

→ From the above, the other solutions are of the form $x = x_0 + \frac{b}{d}t,\ y = y_0 - \frac{a}{d}t,\ t \in \mathbb{Z}$.

→ For a (+ve)-solution, we need t such that $x_0 + \frac{b}{d}t > 0$ and $y_0 - \frac{a}{d}t > 0$.

Case 1: a and b have opposite signs:

Then: if $b > 0$ and $a < 0$, then $t > -\frac{x_0 d}{b}$; $t > \frac{y_0 d}{a}$

for x, y to be > 0. if $b > 0$ and $a > 0$, then $t < -\frac{x_0 d}{b}$; $t > \frac{y_0 d}{a}$

In both case, there are infinite numbers of t's such that $x > 0$, $y > 0$.

Case 2: a and b have the same sign:

Then: for x, y to be both positive, we need

$$-\frac{x_0 d}{b} < t < \frac{y_0 d}{a}$$

(check when both a and b are positive. If both are negative, multiply (1) by -1)

Example. IITDH places an order for some note books totalling Rs. 2490.00, some of which cost Rs. 29 and some costing 33 Rs. How many of each type were ordered?

Soln. Consider the equation $29x+33y=2490$. —(1)

GCD(29, 33) = 1 and by Euclidean algorithm

$33 = 29\times 1 + 4$
$29 = 7\times 4 + 1$

So, $1 = 29 - 7\times 4 = 29 - 7(33-29)$
$= 29\times 8 - 33\times 7$.

Now, $x = 8\times 2490$, $y = -7\times 2490$ is a soln to (1).

The positive corresponds to

$$-\frac{8\times 2490}{33} < t < -\frac{7\times 2490}{29}$$

or

$$-603.6\ldots < t < -601.03\ldots$$

i.e., corresponding to $t=-602$, $t=-603$.

So $\boxed{x=54,\ y=28}$ or $\boxed{x=21,\ y=57}$.

~~7.13 7.14~~

Exe: (To be submitted)

1) Find general solution of the linear Diophantine equation $2072x + 1813y = ~~2849~~ = 2849$.

2) Find all solutions of $19x + 20y = 1909$ with $x > 0, y > 0$.

3) Let $n = \prod_{i=1}^{r} p_i^{s_i}$ be the primary decomposition of n. (Recall that this means $p_1, \dots, p_r$ are distinct primes and $s_i > 0$). Show that every positive divisor of n appears exactly once among the terms when the product $\prod_{i=1}^{r} (1 + p_i + \dots + p_i^{s_i})$.

Deduce that the sum of the divisors of n is

$$\prod_{i=1}^{r} \frac{p_i^{s_i+1} - 1}{p_i - 1}$$

and that the number of divisors of n is $\prod (1 + s_i)$.