Let $p=5$, $f(T) = T^3 - T^2 + 1$, $g(T) = T^2 + 1$

Using Division Algorithm to find the GCD of them.

$$
\begin{array}{r|l}
 & T - 1 \\
\hline
T^2+1 & T^3 - T^2 + 0T + 1 \\
 & T^3 \qquad\quad + T \\
\hline
 & -T^2 - T + 1 \\
 & -T^2 \qquad - 1 \\
\hline
 & -T + 2
\end{array}
$$

$$f(T) = g(T)(T-1) + (-T+2)$$

$$g(T) = (-T+2)(-T-2) + \underline{0}$$

$$
\begin{array}{r|l}
 & -T - 2 \\
\hline
-T+2 & T^2 + 0T + 1 \\
 & T^2 - 2T \\
\hline
 & 2T + 1 \\
 & 2T - 4 \\
\hline
 & 5 \equiv 0 \bmod 5.
\end{array}
$$

GCD is $T - 2$

(If we require GCD to be monic)

Last time:

We have proved the following theorem:

Theorem (Unique prime factorization.)

Let $f(T) \in \mathbb{F}_p[T]$. Then $f(T)$ can be uniquely written as

$$f(T) = c \cdot P_1(T)^{e_1} \cdot P_2(T)^{e_2} \cdot \cdots \cdot P_r(T)^{e_r}$$

where

- c is the leading coefficient of f;
- $P_1, \cdots, P_r$ are monic irreducible polynomials over $\mathbb{F}_p$; and
- $e_1, \cdots, e_r > 0$.

But there are a few lemmas used in the proof not been discussed.

1. Defn. Say f and g are coprime if there are $q_1(T), q_2(T) \in \mathbb{F}_p[T]$ s.t.

$$f(T)q_1(T) + g(T)q_2(T) = \bar{1}.$$

left to you: Prove this is eq to say $GCD(f, g) = \bar{1}$.

2. Lem: If $f \mid h$, $g \mid h$ and f, g are coprime, then $fg \mid h$.

proof. f, g are coprime means $\exists\, q_1, q_2 \in \mathbb{F}_p[T]$ s.t.

$$fq_1 + gq_2 = \bar{1}$$

Hence, $hfq_1 + hgq_2 = h$.

Note that, $f \mid h$ & $g \mid h$, saying $h = q_3 f = q_4 g$.

Then $h = q_4 g f q_1 + q_3 f g q_2 = fg(q_4 q_1 + q_3 q_2)$.

Namely, $fg \mid h$. $\boxtimes$

3 Lem: If f, g are coprime and f, h are coprime, then f, gh are coprime.

Proof. f, g are coprime $\Rightarrow \exists q_1, q_2 \in \mathbb{F}_p[T]$ s.t. $fq_1 + gq_2 = \bar{1}$ ①

f, h are coprime $\Rightarrow \exists q_3, q_4 \in \mathbb{F}_p[T]$ s.t. $fq_3 + hq_4 = \bar{1}$ ②

① $\times h \Rightarrow$ $fhq_1 + ghq_2 = h$ plug in ② :

$$f q_3 + (fhq_1 + ghq_2) q_4 = \bar{1}$$

$$\parallel$$

$$f(q_3 + hq_1q_4) + gh \cdot q_2 q_4 = \bar{1}.$$

Namely, f and gh are coprime.

Coro: If $p_i^{e_i} \mid f$, then $p_1^{e_1} \cdots p_r^{e_r} \mid f$.

Note that: We have $p_i^{e_i}$ coprime to $p_j^{e_j}$ if $p_i \neq p_j$ (monic irr poly)

Next: Roots of a polynomial.

Defn. An element $a \in \mathbb{F}_p$ is called a root of $f(T) \in \mathbb{F}_p[T]$ if $f(a) = \bar{0}$.

4 Prop. $a \in \mathbb{F}_p$ is a root of $f(T) \in \mathbb{F}_p[T]$ if and only if $T - a \mid f(T)$

Proof. Using division algorithm, $\exists\, q, r \in \mathbb{F}_p[T]$ s.t.

$$f(T) = (T-a)\cdot q(T) + r(T) \quad \text{with } \deg r < \deg(T-a) = 1$$

Namely $r(T) = r \in \mathbb{F}_p$.

Now, plug in $a \in \mathbb{F}_p$:

$$f(a) = (a-a)\cdot q(a) + r = 0 + r = r$$

Hence $f(a) = 0 \iff r = 0 \iff f(T) = (T-a)\cdot q(T)$

i.e. $T - a \mid f(T)$.

$\square$

5. Thm. $\#\{\text{roots of } f(T) \text{ in } \mathbb{F}_p\} \leq \deg f$. e.g. $T^{p-1} - \bar{1}$.

Lemma: $T - a$ and $T - b$ are coprime whenever $a \neq b \in \mathbb{F}_p$.

Proof: $(\Rightarrow)$ If $\exists\, q_1, q_2 \in \mathbb{F}_p[T]$ s.t.

$$(T-a)q_1 + (T-b)q_2 = \bar{1},$$

then we have

$$(a-b)q_2(a) = \bar{1}$$

Which means $a-b$ is a unit, hence nonzero. So $a \neq b$.

$(\Leftarrow)$ If $a \neq b$, then $\exists\, c \in \mathbb{F}_p$ s.t. $(a-b)\cdot c = \bar{1}$.

Then $(-c)\cdot(T-a) + c\cdot(T-b) = \bar{1}$

Namely $T-a$ & $T-b$ are coprime.

Proof (of theorem 5):

By prop. 4. $\forall a \in \{\text{roots of } f(T) \text{ in } \mathbb{F}_p\}$, $T-a \mid f(T)$

By the lemma and coro of Lemma 3,

$$\prod_{a \in \{\text{roots of } f(T) \text{ in } \mathbb{F}_p\}} (T-a) \;\Big|\; f(T),$$

degree $= \#\{\text{roots of } f(T) \text{ in } \mathbb{F}_p\}$

Hence,

$$\#\{\text{roots of } f(T) \text{ in } \mathbb{F}_p\} \le \deg f.$$

$\boxtimes$

Recall

$f(T), g(T) \in \mathbb{F}_p[T]$ are nonzero. Then $\deg(fg) = \deg(f) + \deg(g)$.

Rmk: The theorem fails for $\mathbb{Z}/m$, with m composite.

e.g. $m = 8$ and $f(T) = T^2 - \bar{1}$. $\deg f = 2$.

$f(\bar{0}) = \bar{0}^2 - \bar{1} = -\bar{1} \neq \bar{0}$ not a root.

$f(\bar{1}) = \bar{1}^2 - \bar{1} = \bar{0}$ $\bar{1}$ is a root

$f(\bar{2}) = \bar{2}^2 - \bar{1} = \bar{3} \neq \bar{0}$ not a root

$f(\bar{3}) = \bar{3}^2 - \bar{1} = \bar{8} = \bar{0}$ $\bar{3}$ is a root

$f(\bar{4}) = \bar{4}^2 - \bar{1} = -\bar{1} \neq \bar{0}$ not a root

$f(\bar{5}) = \bar{5}^2 - \bar{1} = \overline{24} = \bar{0}$ $\bar{5}$ is a root

$f(\bar{6}) = \bar{6}^2 - \bar{1} = \overline{35} = \bar{3} \neq \bar{0}$ not a root

$f(\bar{7}) = \bar{7}^2 - \bar{1} = \overline{48} = \bar{0}$ $\bar{7}$ is a root.

$\{\text{roots of } f(T)\}$

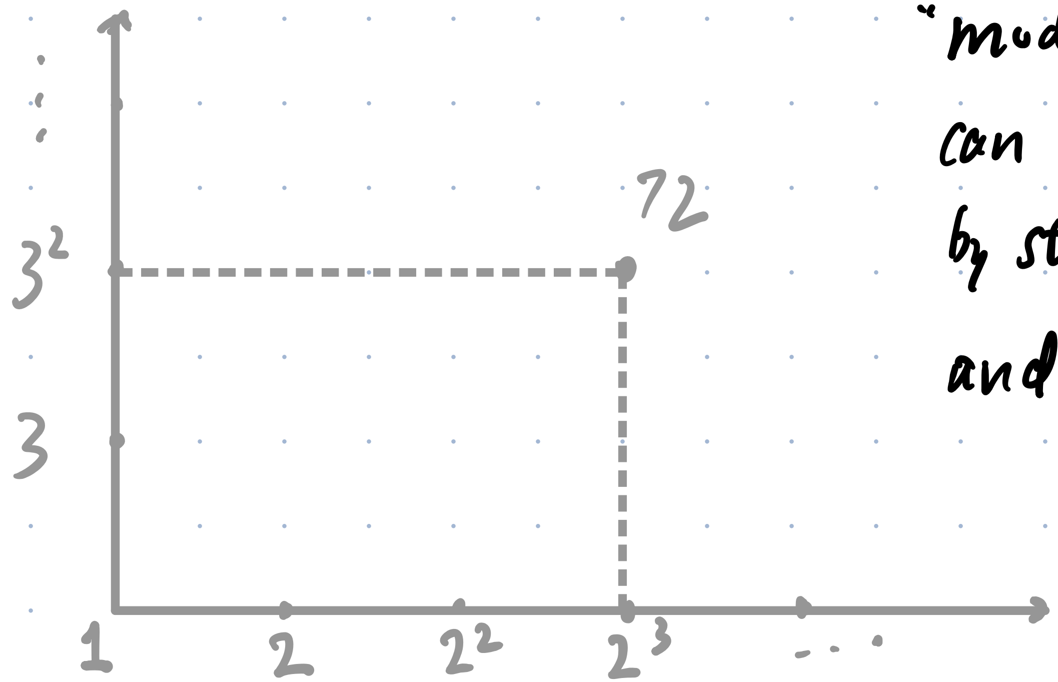
$= \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$

$4 > 2$!!!

Assembling the Modular World.

Each modulus gives us partial information.
In order to get a fuller picture, we want to assemble the information into one.

e.g.

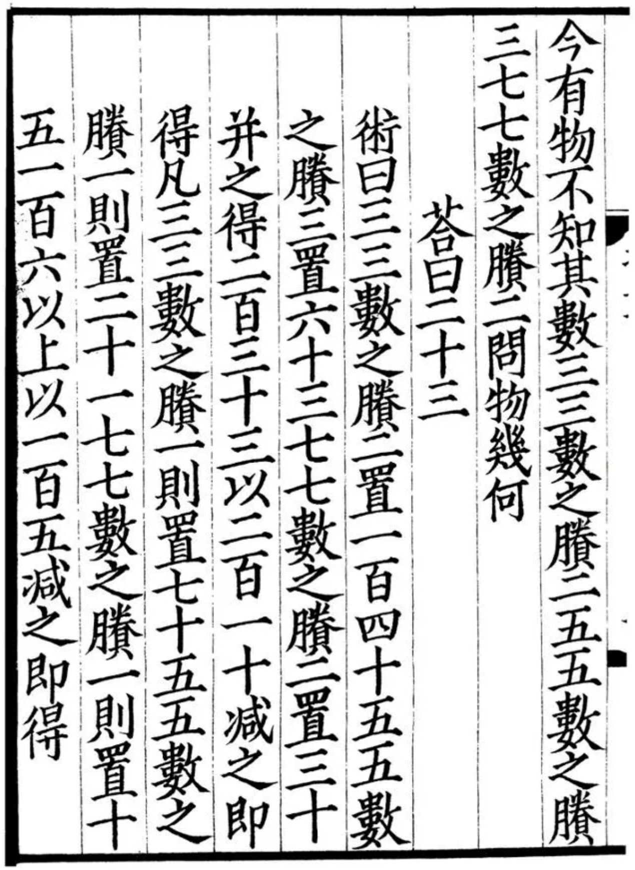


"mod 72" World can be understood by study "mod 3^2" world and "mod 2^3" world.

Ancient Question 物不知數 "certain things whose number is unkown"

(~300–400 A.D., Sun-tzu Suan-ching)

There are certain things whose number is unkown.
If we count them by 3s, we have 2 left over.
If we count them by 5s, we have 3 left over.
If we count them by 7s, we have 2 left over.
How many things are there?



今有物不知其數三三數之賸二五五數之賸
三七七數之賸二問物幾何
荅曰二十三
術曰三三數之賸二置一百四十五五數
之賸三置六十三七七數之賸二置三十
并之得二百三十三以二百一十減之即
得凡三三數之賸一則置七十五五數之
賸一則置二十一七七數之賸一則置十
五一百六以上以一百五減之即得

In the language of number theory, it asks for the solution set

$$\{x \in \mathbb{Z} \mid x \equiv 2 \bmod 3,\ x \equiv 3 \bmod 5,\ x \equiv 2 \bmod 7\}$$

The original answer:

count them by 3s, left over 2 $\rightsquigarrow$ 140 ??

count them by 5s, left over 3 $\rightsquigarrow$ 63 ??

count them by 7s, left over 2 $\rightsquigarrow$ 30 ??

$$\begin{array}{r} 140 \\ 63 \\ 30 \\ \hline 233 \\ -\ 210\ ?? \\ \hline 23 \end{array}$$

210 is a common multiple of 3, 5, 7 $\quad 210 = 2 \cdot 3 \cdot 5 \cdot 7$

140 is a --- ---- of 5, 7 $\quad 140 = 2^2 \cdot 5 \cdot 7$

63 is a --- --- of 3, 7 $\quad 63 = 3 \cdot 3 \cdot 7$

30 is a --- --- of 3, 5 $\quad 30 = 2 \cdot 3 \cdot 5$