HW1 Week 2.

李沛彬 2022111221

Exercise 1.1. *Prove the divisibility rule by 3: an integer is divisible by 3 iff the sum of its digits is divisible by 3.*

Pf: assume there is a n digit number $\overline{a_n a_{n-1} \cdots a_2 a_1}$

$\overline{a_n a_{n-1} \cdots a_2 a_1} = a_n \cdot 10^{n-1} + a_{n-1} \cdot 10^{n-2} + \cdots + a_2 \cdot 10 + a_1$.

$= (a_n + a_{n-1} + \cdots + a_1) + [a_n \cdot \underbrace{9 \cdots 9}_{n-2 \text{ digits}} + a_{n-1} \cdot \underbrace{9 \cdots 9}_{n-3 \text{ digits}} + \cdots + a_2 \cdot 9.]$

the latter part is always divisible by 3. thus $\overline{a_n a_{n-1} \cdots a_2 a_1}$ is divisible by 3. iff $(a_1 + a_2 + \cdots + a_n)$. is divisible by 3.

Exercise 1.2. *Use the Euclidean algorithm to find the GCD and Bézout's coefficients for* $(75, 54)$.

Pf: by Euclidean algorithm.

$75 = 1 \cdot 54 + 21$

$54 = 2 \cdot 21 + 12$

$21 = 1 \cdot 12 + 9$.

$12 = 1 \cdot 9 + 3$.

$9 = 3 \cdot 3 + 0$

$\Rightarrow \gcd(75, 54) = 3$

$3 = 12 - 9 = 12 - (21 - 12) = (54 - 2 \cdot 21) - (21 - (54 - 2 \cdot 21))$

$= 54 - 2 \cdot (75 - 54) - (75 - 54) - (54 - 2 \cdot (75 - 54))$

$= 54 - 2 \cdot 75 + 2 \cdot 54 - (75 - 54) + 54 - 2 \cdot 75 + 2 \cdot 54$

$= 7 \cdot 54 + (-5) \cdot 75$

Exercise 1.3. *Find* $\gcd(2 \cdot 3^{15} + 1, 2 \cdot 3^7 - 5)$.

Pf: by lemma 1.8.

$\gcd(2 \cdot 3^{15} + 1, 2 \cdot 3^7 - 5) = \gcd(2 \cdot 3^{15} + 1 - 3^8 \cdot (2 \cdot 3^7 - 5), 2 \cdot 3^7 - 5)$

$= \gcd(5 \cdot 3^8 + 1, 2 \cdot 3^7 - 5) = \gcd(5 \cdot 3^8 + 1 - 2 \cdot 3^8 + 15, 2 \cdot 3^7 - 5) = \gcd(3^9 + 16, 2 \cdot 3^7 - 5)$

$= \gcd(3^9 + 16 - 3(2 \cdot 3^7 - 5), 2 \cdot 3^7 - 5) = \gcd(3^8 + 31, 2 \cdot 3^7 - 5) = \gcd(3^7 + 36, 2 \cdot 3^7 - 5)$.

$= \gcd(3^7 + 36, -77) = 1$. (we can check $3^7 + 36$ not divisible by 7 or 11 easily).

Exercise 1.4. *If* $\gcd(a, 4) = \gcd(b, 4) = 2$, *find* $\gcd(a + b, 4)$.

Sol: $\gcd(a, 4) = 2 \Rightarrow a = 2(2k_1 + 1)$ $k_1 \in \mathbb{Z}$.

similarly $b = 2(2k_2 + 1)$ $k_2 \in \mathbb{Z}$.

$a + b = 4 \mid k_1 + k_1 + 1)$. $k_1, k_2 \in \mathbb{Z}$. thus $\gcd(a + b, 4) = 4$.

Exercise 1.5. *For every* $a \in \mathbb{Z}$ *find* $\gcd(5a^2 + 2, a - 3)$.

Sol: by lemma 1.8. $\gcd(5a^2 + 2 - 5a(a - 3), a - 3) = \gcd(15a + 2, a - 3) = \gcd(47, a - 3)$.

$\gcd(5a^2 + 2, a - 3) = 1$. for $a \in \mathbb{Z} \setminus \{50, -44\}$.

$\gcd(5a^2 + 2, a - 3) = 47$ for $a \in \{50, -44\}$.

Exercise 2.1. *Solve the equation* $126x - 51y = 9$.

Sol: $\gcd(126, -51) = 3$. $42x + 17(-y) = 3$. (1).

Apply Euclidean Algorithm.

$42 = 17 \cdot 2 + 8$

$17 = 8 \cdot 2 + 1$.

$8 = 8 \cdot 1 + 0$

$1 = 17 - 8 \cdot 2 = 17 - 2(42 - 17 \cdot 2) = (-2) \cdot 42 + 5 \cdot (17)$.

a solution of (1) is $\begin{cases} x_0 = -6 \\ y_0 = -15. \end{cases}$, as well as the solution of the original solution.

$\begin{cases} 126 = 3 \cdot 42 \\ -51 = 3 \cdot -17. \end{cases} \Rightarrow \begin{cases} x = -6 - 17t \\ y = -15 - 42t. \end{cases} \quad t \in \mathbb{Z}$.

Exercise 2.2. *Solve the equation* $2x - 4y + 5z = 3$.

Sol: construct system $\begin{cases} 2x - 4y = a & (1) \\ a + 5z = 3. & (2). \end{cases}$

i/ solve $x - 2y = 1$. one solution is $\begin{cases} x_0 = 5 \\ y_0 = 2. \end{cases}$ the solution for (1) is $\begin{cases} x = \frac{5}{2}a - 2t \\ y = a - t \end{cases}$

ii/ solve $a + 5z = 3$. one solution is $\begin{cases} a = 8 \\ z = -1. \end{cases}$ the solution for (2) is $\begin{cases} a = 8 + 5s \\ z = -1 - s. \end{cases}$

iii/ general solution is: $\begin{cases} x = \frac{5}{2}(8 + 5s) - 2t = 20 + \frac{25}{2}s - 2t \\ y = 8 + 5s - t = 8 + 5s - t \\ z = -1 - s \end{cases}$

Exercise 2.3. *Solve the system*

$$\begin{cases} 4x + 5y + 7z = 2 & (1) \\ 7x - 2y + 3z = -1 & (2). \end{cases}$$

Sol: $(2) \cdot \frac{5}{2} + (1)$ $\frac{43}{2}x + \frac{29}{2}z = -\frac{1}{2}$. $\Rightarrow$ $43x + 29z = -1$. (3).

one of the solution of (3) is $\begin{cases} x_0 = 2 \\ z_0 = -3. \end{cases}$, the solution of (3). $\begin{cases} x = 2 + 29t \\ z = -3 - 43t. \end{cases}$

Substitute x and z by expression w.r.t. t, in (1). $8 + 116t + 5y - 21 - 301t = 2$. $\Rightarrow$ $y = 3 + 37t$

thus. the general sol. is. $\begin{cases} x = 2 + 29t \\ y = 3 + 37t \\ z = -3 - 43t \end{cases}$

Exercise 2.4. *Let* $a, b, c, n \in \mathbb{Z}$, $a, b, c \neq 0$ *and* $d = \gcd(a, b, c)$. *Show that the equation* $ax + by + cz = n$ *has an integer solution if and only if* $d \mid n$.

Pf: "$\Rightarrow$" denote the integer solution by (x_0, y_0, z_0)

since $d \mid a$, $d \mid b$, $d \mid c$. $d \mid ax + by + cz$. for any integer x, y, z.

$n = ax_0 + by_0 + cz_0$. thus. $d \mid n$.

"$\Leftarrow$" since $d \mid n$. denote $n = dn'$

by Bezout identity. there exist integer solution. of equation $ax' + by' + cz' = d$. denote them by (x_1, y_1, z_1).

multiple the both side by n'. $ax_1n' + by_1n' + cz_1n' = n$.

i.e. the original equation has integer solution $\begin{cases} x = x_1n' \\ y = y_1n' \\ z = z_1n' \end{cases}$

HW 2. Week 3.

Exercise 3.1. *Find the canonical representation of* 12000.

$12000 = 2^3 \cdot 1500 = 2^5 \cdot 375 = 2^5 \cdot 3^1 \cdot 125 = 2^5 \cdot 3^1 \cdot 5^3$

Exercise 3.2. *Prove that* $a^3 \mid b^2$ *implies* $a \mid b$

Pf: Assume $a = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$ $\quad b = p_1^{t_1} p_2^{t_2} \cdots p_s^{t_s}$.

$a^3 \mid b^2$ implies $3k_i \le 2t_i$ for all $i = 1, \cdots s$. by Prop. 3.3.

k_i, t_i are positive integer $\quad 3k_i \le 2t_i \Rightarrow k_i \le \frac{2}{3} t_i \le t_i$ for all i. $\Rightarrow$ $a \mid b$ by prop. 3.3.

Exercise 3.3. *Prove that if* ab, bc, ac *are integer cubes then* a, b, c *are integer cubes.*

Pf: $ab = p_1^{3k_1} \cdots p_s^{3k_s}$ $\quad k_i, l_i, m_i = 0, 1, 2, \cdots$

$bc = p_1^{3l_1} \cdots p_s^{3l_s}$

$ac = p_1^{3m_1} \cdots p_s^{3m_s}$.

$abc = p_1^{\frac{3}{2}(k_1+l_1+m_1)} \cdots p_s^{\frac{3}{2}(k_s+l_s+m_s)}$, since $a, b, c \in \mathbb{Z}$, $\frac{1}{2}(k_i + l_i + s_i) \in \mathbb{Z}$

since $bc \mid ab \cdot ac$. i.e. $p_1^{3l_1} \cdots p_s^{3l_s} \mid p_1^{3(k_1+m_1)} \cdots p_s^{3(k_s+m_s)}$, that is $l_i \le k_i + m_i$ for all i. by.

$a = \frac{abc}{bc} = p_1^{\frac{3}{2}(k_1+m_1-l_1)} \cdots p_s^{\frac{3}{2}(k_s+m_s-l_s)}$. $\quad \frac{k_i - l_i + s_i}{2} = \frac{k_i + l_i + s_i}{2} - l_i \in \mathbb{Z}_+ \cup \{0\}$.

a is cube of $p_1^{\frac{k_1+m_1-l_1}{2}} \cdots p_s^{\frac{k_s+m_s-l_s}{2}}$, which is proved to be an integer above. Similarly for b, c.

Exercise 3.4. *Let* a, n *be positive integers. Prove that* $\sqrt[n]{a} \in \mathbb{Q}$ *implies* $\sqrt[n]{a} \in \mathbb{Z}$.

Pf: $\sqrt[n]{a} \in \mathbb{Q}$ assume $\sqrt[n]{a} = \frac{p}{q}$ p, q are coprime $\Rightarrow a = \frac{p^n}{q^n} \in \mathbb{Z}_+$. $\Rightarrow q^n \mid p^n \Rightarrow q = 1$. prop. 3.3.

thus. $a = p^n$. $\sqrt[n]{a} = p \in \mathbb{Z}$.

Exercise 4.1. *Solve the system*

$$\begin{cases} x \equiv 2 \pmod 5 \\ x \equiv 1 \pmod 6 \\ x \equiv 3 \pmod 7 \end{cases}.$$

Hint. Let x_0 be a solution of the system

$$\begin{cases} x \equiv 2 \pmod 5 \\ x \equiv 1 \pmod 6 \end{cases}. \quad (1)$$

Then solve the system

$$\begin{cases} x \equiv x_0 \pmod{30} \\ x \equiv 3 \pmod 7 \end{cases}. \quad (2).$$

Sol: $\begin{cases} x = 5y + 2 \\ x = 6z + 1 \end{cases} \Rightarrow 5y - 6z = -1.$

particular sol: $\begin{cases} y_0 = -5 \\ z_0 = -4 \end{cases}$

solution of (1) $x_0 = -23 + 30t$.

$\begin{cases} x = -23 + 30t \\ x = 3 + 7s. \end{cases} \Rightarrow 30t - 7s = 26.$

a particular sol. $\begin{cases} t = 6 \\ s = 22 \end{cases}$

thus the sol. for system (2): $x_1 = 157 + 210r$. $r \in \mathbb{Z}$.

Exercise 4.2. *Is the system*

$$\begin{cases} x \equiv 1 \pmod{30} \\ x \equiv -5 \pmod{21} \\ x \equiv 16 \pmod{35} \end{cases}.$$

solvable?

Sol: Since 30, 21, 35 not coprime. we can't use Chinese Remainder Theorem directly.

$\begin{cases} x = 1 + 30a \\ x = -5 + 21b \\ x = 16 + 35c \end{cases}$ eliminate x. $\longrightarrow \begin{cases} 30a - 21b = -6 \\ 30a - 35c = 15. \\ 21b - 35c = 21 \end{cases} \Rightarrow \begin{cases} 10a - 7b = -2 \\ 6a - 7c = 3 \\ 3b - 5c = 3 \end{cases}$

find a particular sol: $\begin{cases} a = 4 \\ b = 6 \\ c = 3. \end{cases}$ and $\det A = 0$.

so it's solvable and have infinite many. sol. such as $x = 121$.

Exercise 5.1. *Compute* $\varphi(60)$.

Pf: $60 = 2^2 \cdot 3^1 \cdot 5^1$

by coro 3.4. $\varphi(60) = 2^1 \cdot 1 \cdot 3^0 \cdot (3-1) \cdot 5^0 \cdot (5-1) = 2 \cdot 2 \cdot 4 = 16$.

Exercise 5.2. *Show that* $\varphi(n)$ *is even for every* $n \geq 3$.

Pf: if n is prime. than $\varphi(n) = n-1$. (prime ≥ 3 is odd. $n-1$ is even).

if n is not prime. let $n = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$ be it's canonical representation. By coro 5.4.

$\varphi(n) = p_1^{k_1-1}(p_1-1) \cdots p_s^{k_s-1}(p_s-1)$. one of the factor be even, then $\varphi(n)$ is even.

if only prime divisor is $p_1 = 2$. then $p_1^{k_1-1}$ is even.

if there exist other prime divisor, p_i. then $p_i - 1$ is even.

Exercise 5.3. *Prove the identity* $\sum_{d|n} \varphi(d) = n$ *by induction on* n.

Hint. Choose a prime divisor p of n and write $n = mp^k$ for m coprime p, then use the induction assumption for m.

Pf: (1). $n=1$. $\varphi(1) = 1$. holds.

(2) Assume $\sum_{d|m} \varphi(d) = m$ for all $m < n$

(3). consider n.

i/ n is prime. $\sum_{d|n} \varphi(d) = \sum_{1|n} \varphi(1) + \sum_{n|n} \varphi(n) = 1 + n - 1 = n$

ii/ n is power of some prime. let $n = p^k$. for $i < k$. $\sum_{d|p^i} \varphi(d) = p^i$

$\sum_{d|p^k} \varphi(p^k) = \sum_{i=0}^{k} \varphi(p^i) = 1 + \sum_{i=1}^{k} p^{i-1}(p-1) = 1 + p - 1 + p^2 - p + \cdots + p^k - p^{k-1} = p^k$

iii/ $n = mp^k$. $\gcd(m, p^k) = 1$. $m \neq 1$. since $m < n$ and $p^k < n$. we have $\sum_{d|m} \varphi(d) = m$, $\sum_{d|p^k} \varphi(d) = p^k$

By thm5.3. $\varphi(n) = \varphi(m) \cdot \varphi(p^k) = m \cdot p^k = n$.

Exercise 6.1. *Find* $10^{200} \pmod{91}$

Sol: Firstly find $10^{200} \pmod 7$ and $10^{200} \pmod{13}$.

$10^{200} \equiv 3^{200} = 9^{100} \equiv 2^{100} \equiv 16^{25} \equiv 2^{25} \equiv 32^5 \equiv 4^5 \equiv 1024 \equiv 2 \pmod 7$.

$10^{200} \equiv 100^{100} \equiv 9^{100} \equiv 81^{50} \equiv 3^{50} \equiv 243^{10} \equiv 9^{10} \equiv 81^5 \equiv 3^5 \equiv 243 \equiv 9 \pmod{13}$.

then find $\begin{cases} x \equiv 2 \mod 7 \\ x \equiv 9 \mod 13. \end{cases} \Rightarrow \begin{cases} x = 2 + 7y \\ x = 9 + 13z \end{cases} \Rightarrow 7y - 13z = 7$ a particular solution. $\begin{cases} y = 14. \\ z = 7 \end{cases}$

$\Rightarrow$ sol. $x = 100 + 91t = 9 + 91t$.

thus $10^{200} \pmod{91} \equiv 9$.

Exercise 6.2. *Prove that*

1. $43^{101} + 23^{101}$ *is divisible by 66*
2. $2^{70} + 3^{70}$ *is divisible by 13.*

Pf: 1. $43^{101} \equiv 1^{101} \equiv 1 \pmod 6$

$43^{101} \equiv 10^{101} = 100^{50} \cdot 10 \equiv 1^{50} \cdot 10 \equiv 10 \pmod{11}$

$23^{101} \equiv 5^{101} \equiv 25^{50} \cdot 5 \equiv 1^{50} \cdot 5 = 5 \pmod{11}$

$23^{101} \equiv 1^{101} \equiv 1 \pmod{11}$

find solution : $\begin{cases} x = 1 + 6x_1 \\ x = 10 + 11x_2 \end{cases} \Rightarrow 6x_1 - 11x_2 = 9$ particular sol. $\begin{cases} x_1 = 7 \\ x_2 = 3 \end{cases} \Rightarrow 43^{101} \bmod 66 = 43.$

$\begin{cases} y = 5 + 6y_1 \\ y = 1 + 11y_2 \end{cases} \Rightarrow 6y_1 - 11y_2 = -4$ particular sol. $\begin{cases} y_1 = 21 \\ y_2 = 8 \end{cases} \Rightarrow 23^{101} \bmod 66 = 23$

$43^{101} + 23^{101} \equiv 43 + 23 \equiv 0 \pmod{66}$

2. $2^{70} \equiv 32^{14} \equiv 6^{14} \equiv 36^7 \equiv 10^7 \equiv 9^3 \cdot 10 \equiv 3 \cdot 12 \equiv 10. \pmod{13}$

$3^{70} \equiv 243^{14} \equiv 9^{14} \equiv 81^7 \equiv 3^7 \equiv 27 \cdot 81 \equiv 1 \cdot 3 \equiv 3. \pmod{13}$.

Thus $2^{70} + 3^{70} \equiv 0 \pmod{13}$.

Exercise 6.3. *Prove that if $a^2 + b^2$ is divisible by 7 then $a^2 + b^2$ is divisible by 49.*

Pf: consider $a^2 \bmod 7$. we have:

a	0	1	2	3	4	5	6
$a^2 \bmod 7$	0	1	4	2	2	4	1

we know $8^2 \equiv 1^2 \equiv 1 \pmod 7$, $9^2 \equiv 2^2 \equiv 4 \pmod 4$ ...

Thus the possible cases for $a^2 \bmod 7$ is $\{0, 1, 2, 4\}$.

consider $(a^2+b^2) \bmod 7$. the only case for $a^2 + b^2 \equiv 0 \pmod 7$ is $\begin{cases} a^2 \equiv 0 \pmod 7 \\ b^2 \equiv 0 \pmod 7 \end{cases}$

By prop. 3.1. $7 \mid a^2$ implies $7 \mid a$. thus. $49 \mid a^2$. Similarly $49 \mid b^2$. Thus $49 \mid (a^2+b^2)$

Exercise 6.4. *Find* $7^{120} \pmod{19 \cdot 23}$.

Sol: since 7 and 19. 7 and 23 are co-prime

$\begin{cases} \varphi(19) = 18 \\ \varphi(23) = 22. \end{cases}$ the Euler thm. implies $\begin{cases} 7^{18} \equiv 1 \mod (19) \\ 7^{22} \equiv 1 \mod (23) \end{cases}$

$7^{120} \equiv (7^{18})^6 \cdot 7^{12} \equiv 7^{12} \equiv 49^6 \equiv 11^6 \equiv 121^3 \equiv 7^3 \equiv 1 \pmod{19}$

$7^{120} \equiv (7^{22})^5 \cdot 7^{10} \equiv 7^{10} \equiv 49^5 \equiv 3^5 \equiv 13 \pmod{23}$

by Chinese remainder thm. solve $\begin{cases} x = 1 + 19y \\ x = 13 + 23z \end{cases} \Rightarrow 19y - 23z = 12.$ a particular sol. is $\begin{cases} y_0 = -3 \\ z_0 = -3. \end{cases}$

thus $7^{120} \pmod{19 \cdot 23} \equiv -56 \equiv 381$

Exercise 6.5. *Find* $14^{100} \pmod{34}$. *Notice that Euler's theorem can not be directly applied.*

$14^{100} \bmod 34 \Leftrightarrow 2^{100} \cdot 7^{100} \bmod (2 \cdot 17)$.

1). find $2^{100} \cdot 7^{100} \bmod 2. = 0$

2) find $2^{100} \cdot 7^{100} \bmod 17$. 2, 7 and 17 are co-prime

$\varphi(17) = 16$. the Euler's thm implies $\begin{cases} 2^{16} \equiv 1 \pmod{17} \\ 7^{16} \equiv 1 \pmod{17} \end{cases}$

$2^{100} \equiv (2^{16})^6 \cdot 2^4 \equiv 16 \pmod{17}$

$7^{100} \equiv (7^{16})^6 \cdot 7^4 = 49^2 \equiv 15^2 \equiv 4 \pmod{17}$. $\Rightarrow 2^{100} \cdot 7^{100} \equiv 16 \cdot 4 \equiv 13 \pmod{17}$.

3) solve $\begin{cases} x = 2y \\ x = 13 + 17z \end{cases} \Rightarrow 2y - 17z = 13. \Rightarrow$ a particular sol. $\begin{cases} y = 15 \\ z = 1. \end{cases}$

Thus. $14^{100} \equiv 30 \pmod{34}$.

Exercise 6.6. *Solve the equation $x^{99} + x^{71} + 2x^{49} + x^{20} + \bar{1} = \bar{0}$ in $\mathbb{Z}/11\mathbb{Z}$*

Sol: $\varphi(11) = 10$. we have $a^{10} \equiv 1 \pmod{11}$ for all $a = [1:10]$ since 11 is prime.

the original equation is equivalent to $x^9 + x + 2x^9 + \bar{2} = \bar{0}$

Also since 11 is prime. $\forall a \in \mathbb{Z}/11\mathbb{Z} \setminus \{\bar{0}\}$, a is invertible. we can check $\bar{0}$ is not a sol.

thus the equation is equivalent to $x^2 + \bar{2}x + \bar{3} = 0 \Leftrightarrow x^2 + \bar{2}x - \bar{8} = 0 \Leftrightarrow (x + \bar{4})(x - \bar{2}) = 0$

$\Rightarrow$ the solution is $x = \bar{2}$ and $x = 7$

HW3. Week 4

Exercise 6.7. *Find all integer x satisfying $8x^2 - 7x + 17 \equiv 0 \pmod{105}$.*

Sol: the congruence is equivalent to the system.

$$\begin{cases} 8x^2-7x+17 \equiv 0 \pmod 3 \\ 8x^2-7x+17 \equiv 0 \pmod 5 \\ 8x^2-7x+17 \equiv 0 \pmod 7 \end{cases}$$

$\bar{x} = \frac{\bar{7} \pm \sqrt{\bar{-495}}}{\bar{16}} = \frac{\bar{1}}{\bar{1}} = \bar{1}$ (in $\mathbb{Z}/3\mathbb{Z}$)

$\bar{x} = \frac{\bar{7} \pm \sqrt{\bar{-495}}}{\bar{16}} = \frac{\bar{2}}{\bar{1}} = \bar{2}$ (in $\mathbb{Z}/5\mathbb{Z}$)

$\bar{x} = \frac{\bar{7} \pm \sqrt{\bar{-495}}}{\bar{16}} = \frac{\sqrt{\bar{2}}}{\bar{2}} = \frac{\pm\bar{4}}{\bar{2}} = \pm\bar{4}\cdot\bar{4} = \bar{2}$ or $\bar{5}$ (in $\mathbb{Z}/7\mathbb{Z}$)

$x = \frac{7 \pm \sqrt{49 - 4\cdot 8\cdot 17}}{16} = \frac{\bar{7} \pm \sqrt{\bar{-495}}}{\bar{16}}$.

then solve the system $\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 2 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases}$ and $\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 2 \pmod 5 \\ x \equiv 5 \pmod 7 \end{cases}$

$\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 2 \pmod 5 \end{cases} \Rightarrow \begin{cases} x = 1+3y \\ x = 2+5z \end{cases} \Rightarrow 3y - 5z = 1 \Rightarrow \begin{cases} y = 2 \\ z_1 = 1 \end{cases} \Rightarrow x = 7 + 15t_1$

i) $\begin{cases} x \equiv 7 \pmod{15} \\ x \equiv 2 \pmod 7 \end{cases} \Rightarrow \begin{cases} x = 7+15y \\ x = 2+7z \end{cases} \Rightarrow 7z - 15y = 5 \Rightarrow \begin{cases} y_2 = 2 \\ z_2 = 5 \end{cases} \Rightarrow x = 37 + 105t_2$

ii) $\begin{cases} x \equiv 7 \pmod{15} \\ x \equiv 5 \pmod 7 \end{cases} \Rightarrow \begin{cases} x = 7+15y \\ x = 5+7z \end{cases} \Rightarrow 7z - 15y = 2 \Rightarrow \begin{cases} y_3 = 5 \\ z_3 = 11 \end{cases} \Rightarrow x = 82 + 105t_3$.

thus $x \equiv 37, 82 \pmod{105}$

Exercise 6.8. *Find all integer x satisfying $x^2 \equiv 59 \pmod{125}$.*

Hint. Follow the proof of Proposition 6.8.

若在四更复杂. 算完 mod 5 之后可将 $x = x_0 + 5y$. 代入原式 $(\bmod 5^3)$. 求 y.

Sol: by Prop 6.8. the equation has exactly 2 solution.

1) firstly find $x^2 \equiv 59 \pmod 5$. $\Rightarrow x^2 \equiv 4 \pmod 5$. $\Rightarrow x = 2$ or $x = 3 \pmod 5$.

2) $a^2 - 59 = k_1 \cdot 5$, put $a' = a + 5c$ and $a'^2 \equiv 59 \pmod{5^2}$. when $k_1 + 2ac \equiv 0 \pmod 5$. by proof of Prop 6.8.

i) $a = 2$. $k_1 = -11$. $c = 4$ $\Rightarrow a' = 22$.

ii) $a = 3$. $k_1 = -10$ $c = 0$ $\Rightarrow a' = 3$.

3) $a'^2 - 59 = k_2 \cdot 25$, put $a'' = a' + 25c$ and $(a'')^2 \equiv 59 \pmod{5^3}$ when $k_2 + 2a'c \equiv 0 \pmod 5$.

i) $a' = 22$. $k_2 = 17$ $c = 2$ $\Rightarrow a'' = 72$.

ii) $a' = 3$. $k_2 = -2$. $c = 2$ $\Rightarrow a'' = 53$.

The final solution is $x = 72$ or 53.

Exercise 7.1. i) *Find the least primitive root modulo 41.*
ii) *Prove that there is no primitive root modulo 12.*

i). $\varphi(41) = 40 = 2^3 \cdot 5^1$ a is a primitive root modulo 41 $\Leftrightarrow a^8 \not\equiv 1$. and $a^{20} \not\equiv 1$. $(\bmod 41)$

test. $2^{20} \equiv (1024)^2 \equiv 40^2 \equiv 1$. $(\bmod 41)$. $2^8 \equiv 2^6 \cdot 2^2 \equiv 23 \cdot 4 \equiv 10$

不能跳合数. 不是同时 mod = 1

test $3^{20} \equiv 81^5 \equiv 40^5 \equiv 40 \pmod{41}$ $3^8 \equiv 81^2 \equiv 40^2 \equiv 1 \pmod{41}$.

test $5^{20} \equiv 625^5 \equiv 10^5 \equiv 1 \pmod{41}$. $6^{20} \equiv (-1)$. $6^8 \equiv 10$.

test $7^{20} \equiv 49^{10} \equiv 8^{10} \equiv 2^{30} \equiv 2^{10} \equiv 40$. $(\bmod 41)$. ✗ $7^8 \equiv 49^4 \equiv 8^4 \equiv 2^{12} \equiv 40 \cdot 2^2 \equiv 37 \pmod{41}$.

Thus, 7 is the least primitive root mod 41.

ii). Pf: it's equivalent to show $(\mathbb{Z}/12\mathbb{Z})^*$ has no generator. i.e. $\nexists a \in \mathbb{Z}/12\mathbb{Z}$ s.t. $\operatorname{ord} a = \varphi(12) = 4$.

consider the generate subgroup. $\langle \bar{5} \rangle = \{\bar{5}, \bar{1}\}$. $\langle \bar{7} \rangle = \{\bar{7}, \bar{1}\}$. $\langle \bar{11} \rangle = \{\bar{1}, \bar{11}\}$.

thus $\operatorname{ord}(\bar{11}) = \operatorname{ord}(\bar{5}) = \operatorname{ord}(\bar{7}) = 2 \neq 4$. no generator.

Exercise 7.2. *Let $g \in \mathbb{Z}$ be a primitive root modulo n and $h \in \mathbb{Z}, gh \equiv 1 \mod n$. Show that h is a primitive root modulo n.*

Pf: $gh \equiv 1 \mod n$ implies $\bar{h} = \bar{g}^{-1}$ in $(\mathbb{Z}/n\mathbb{Z})^*$.

by Modern Algebra 's course. we have $\operatorname{ord}(\bar{h}) = \operatorname{org}(\bar{g}) = |(\mathbb{Z}/n\mathbb{Z})^*|$

That is, h is a generator of $(\mathbb{Z}/n\mathbb{Z})^*$. i.e. a primitive root modulo n.

Exercise 7.3. *Let p be an odd prime. Prove that*

$$1^n + 2^n + \cdots + (p^2-1)^n \equiv \begin{cases} 0 \pmod{p^2}, & \text{if } p-1 \nmid n \\ -p \pmod{p^2}, & \text{if } p-1 \mid n \end{cases}$$

Hint. Follow the proof of Problem 7.7. If g is a primitive root modulo p^2 and $p-1 \nmid n$ then $g^n \not\equiv 1 \pmod{p}$.

Pf: by prop. 7.6. there always exists primitive root modulo p^2. denote it by g.

$\varphi(p^2) = p(p-1)$

$1^n + 2^n + \cdots + (p^2-1)^n \equiv (g^0)^n + (g^1)^n + \cdots + (g^{p^2-p-1})^n$

i) if $p-1 \nmid n$. then $p^2-p \nmid n$. $g^n \not\equiv 1 \mod p^2$.

$$LHS \equiv \frac{(g^n)^{p^2-p}-1}{g^n-1} \equiv \frac{1-1}{g^n-1} \equiv 0 \pmod{p^2}$$

ii) if $p-1 \mid n$ then $(p-1)p \mid np$ $g^{np} \equiv 1 \pmod{p^2}$.

so we have $g^{n(p+1)} \equiv g^n \pmod{p^2}$. $LHS \equiv p \cdot \sum_{k=0}^{p-2} (g^k)^n$

by pro 7.9. $\sum_{k=0}^{p-2} (g^k)^n \equiv -1 \mod p$ i.e. $\sum_{k=0}^{p-2} (g^k)^n = -1 + kp$.

Thus $LHS \equiv p(kp-1) \equiv -p \pmod{p^2}$.

mod $p^2=0$

$n \geq 2$. trivial

$n=1$. $= p \cdot \frac{p(p-1)}{2} \mid p^2$

$1^2 + 2^2 + \cdots + (p^2-1)^2 \equiv 1\sum (g_i)^n + 1^n + (2p)^n + \cdots (p(p-1))^n \pmod{p^2}$

$(1-g^n)\left(\sum_{i=0}^{p^2-p-1} (g^n)^i\right) = 1 - (g^n)^{p(p-1)} \equiv 0 \pmod{p^2}$.

⇒ 要证这个整除 p^2 需要 $1-g^n$ 与 p 互质 (不是与 p^2)

i) $p-1 \nmid n$. $\Rightarrow g^n \not\equiv 1 \pmod{p}$.

consider inverse - negative prop.

$g^n \equiv 1 \pmod{p} \Rightarrow p-1 \mid n$. g是$p^2$的原根. 是p的原根.

ii) $p-1 \mid n$. $\Rightarrow n = (p-1)k$.

$(g^k)^{p-1} \equiv 1 \pmod{p} \Rightarrow (g^k)^{p-1} = 1 + ps$. (原根.)

$\sum_{i=0}^{p^2-p-1} \left((g^k)^{p-1}\right)^i = \sum_{i=0}^{p^2-p-1} (1+ps)^i \equiv \sum_{i=0}^{p^2-p-1} (1+ips) \mod p^2$

$= p(p-1) + ps \cdot \frac{p(p-1)(p^2-p-1)}{2} = -p$.

HW 4. Week 5.

Exercise 8.1. *Prove that*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, \text{ if } p \equiv 1 \pmod 4 \\ -1, \text{ if } p \equiv 3 \pmod 4 \end{cases}$$

pf: since $(p,-1)=1$ for any prime p. by Euler's criterion $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \bmod p$.

if $p \equiv 1 \pmod 4$ then $4 \mid p-1$, $2 \mid \frac{p-1}{2}$. $(-1)^{\frac{p-1}{2}} \equiv 1 \pmod p$

if $p \equiv 3 \pmod 4$. then $(p-1) \equiv 2 \pmod 4$. $\frac{p-1}{2} \equiv 1 \pmod 2$. thus $(-1)^{\frac{p-1}{2}} \equiv -1 \bmod p$.

Exercise 8.2. *Let $p > 3$ be a prime. Prove that the sum of quadratic residues modulo p in the interval $[1, p-1]$ is divisible by p.*

Hint. Multiply all the residues by an integer $a \not\equiv 0, \pm 1 \pmod 3$.

pf: by lemma 8.1. $\forall a \in [1, p-1]$. if a is a quadratic residue. modulo p. then $x^2 \equiv a \pmod p$ has 2 solution.

since p is prime. $(a,p)=1$. ; in $\{1, 2, \dots, p-1\}$. there are $\frac{p-1}{2}$ quadratic residue. and $\frac{p-1}{2}$ number nonresidue.

$S = \frac{1}{2}(1^2 + 2^2 + \cdots + (p-1)^2) = \frac{1}{2} \cdot \frac{(p-1)p(2p-1)}{6}$

since p is prime. $2 \nmid p$. $6 \nmid p$. thus. $p \mid S$.

HW5 Week 6.

Exercise 8.3. *Compute* $(\frac{41}{151}), (\frac{43}{151})$.

$41 \equiv 1 \mod 4$ $\quad 41 \equiv 151 \equiv 3 \pmod 4$. $\quad 43 \equiv 3 \pmod 8$

7 has quadratic residue 1, 2, 4

$$(\frac{41}{151}) = (\frac{151}{41}) = (\frac{28}{41}) = (\frac{4}{41})\cdot(\frac{7}{41}) = (\frac{7}{41}) = (\frac{41}{7}) = (\frac{6}{7}) = \frac{2}{7}\cdot\frac{3}{7} = 1\cdot(-1) = -1.$$

$$(\frac{43}{151}) = -(\frac{151}{43}) = -(\frac{22}{43}) = -(\frac{2}{43})\cdot(\frac{11}{43}) = (-1)\cdot(-1)\cdot -(\frac{43}{11}) = -(\frac{-1}{11}) = (-1)\cdot(-1) = 1$$

$11 \equiv 3 \pmod 4$ by exercise 8.1

Exercise 8.4. *Show that* $166 \mid 13^{41} + 1$.

Hint. Use Euler's criterion.

Pf: $166 = 2 \times 83$

it suffices to show that. $2 \mid 13^{41}+1$, $83 \mid 13^{41}+1$, $2 \mid 13^{41}+1$ is trivial since $13^{41}+1$ is even.

$83 = 41\times 2 + 1$. by Euler's criterion $a^{\frac{p-1}{2}} = (\frac{a}{p}) \bmod p$ when $p \nmid a$.

$13^{41} \equiv -1 \pmod{83}$ since $(\frac{13}{83}) = (\frac{83}{13}) = (\frac{5}{13}) = (\frac{13}{5}) = (\frac{3}{5}) = -1$. i.e. 13 is quadratic non-residue modulo 83.

i.e. $83 \mid 13^{41}+1$

Exercise 8.5. *Show that 3 is a quadratic residue modulo prime p iff* $p \equiv \pm 1 \mod 12$.

Pf: by Quadratic Residue law. $(\frac{3}{p}) = \begin{cases} -(\frac{p}{3}) & \text{if } p \bmod 4 = 3. \\ (\frac{p}{3}). & \text{if } p \bmod 4 = 1. \end{cases}$ ($\bmod 4 = 2$ is impossible for odd prime).

1 are quadratic residue module 3. ; 2 is quadratic non-residue modulo 3.

$$\begin{cases} p \equiv 1 \pmod 3. \text{ and } p \equiv 1 \pmod 4 \Rightarrow p \equiv 1 \pmod{12}. \\ p \equiv 2 \pmod 3. \text{ and } p \equiv 3 \pmod 4 \Rightarrow p \equiv -1 \pmod{12}. \end{cases}$$

Exercise 8.6. *Prove that* $(\frac{-3}{p}) = (\frac{p}{3})$ *for any odd prime* p.

Pf: by Ex 8.1 $(\frac{-1}{p}) = \begin{cases} 1 & p \equiv 1 \ (4) \\ -1 & p \equiv 3 \ (4) \end{cases}$

i/ $p \equiv 3 \ (4)$.

$(\frac{-3}{p}) = (\frac{-1}{p})(\frac{3}{p}) = (-1)\cdot -(\frac{p}{3}) = (\frac{p}{3})$.

ii/ $p \equiv 1 \ (4)$

$(\frac{-3}{p}) = (\frac{-1}{p})(\frac{3}{p}) = 1\cdot(\frac{p}{3}) = (\frac{p}{3})$

since p is odd prime. i/, ii/ constructs the complete case.

Exercise 9.1. *Find the remainder of* 90! *divided by* 97.

Hint. Use Wilson's Theorem.

Sol: by Wilson's thm. $96! \equiv -1 \pmod{97}$ since 97 is a prime.

$96\cdot 95\cdot 94\cdot 93\cdot 92\cdot 91 \equiv 6! \equiv 41 \pmod{97}$.

Since $(41, 97) = 1$.

$97 = 2\cdot 41 + 15$

$41 = 2\cdot 15 + 11$

$15 = 1\cdot 11 + 4$

$11 = 2\cdot 4 + 3$.

$4 = 1\cdot 3 + 1$

$3 = 1\cdot 3 + 0$.

$1 = 4-3 = (15-11) - (11-2\cdot 4) = 15 - 11 - 11 + 2\cdot(15-11) = 3\cdot 15 + (-4)\cdot 11 = 3\cdot(97 - 2\cdot 41) + (-4)\cdot(41 - 2\cdot 15) = 3\cdot 97 - 10\cdot 41 + 8\cdot(97 - 2\cdot 41)$

$= 11\cdot 97 - 26\cdot 41$

thus. $(41)^{-1} \equiv 71 \pmod{97}$.

$90! \equiv (96!)\cdot(41)^{-1} \equiv (-1)\cdot 71. \equiv 26 \pmod{97}$

Exercise 9.2. *Prove that 641 is a factor of F_5.* *Hint.* Use the identities $641 = 27 \cdot 5 + 1$ and $641 = 2^4 + 5^4$.

$F_5 = 2^{2^5} + 1. = 2^{32} + 1.$ $641 \mid 2^{32}+1$ is equivalent to $2^{32} \equiv -1 \pmod{641}$.

$641 = 2^7 \cdot 5 + 1 \Rightarrow 2^7 \cdot 5 \equiv -1 \pmod{641} \Rightarrow 2^{28} \cdot 5^4 \equiv 1 \pmod{641}$.

$641 = 2^4 + 5^4 \Rightarrow 5^4 \equiv -2^4 \pmod{641}$.

$2^{32} \equiv 2^{28} \cdot 2^4 \equiv 2^{28} \cdot -5^4 \equiv -1 \pmod{641}$. thus. $641 \mid F_5$.

HW 6. Week 7.

无通解. 可对具体区间 判定提高概率的方法.

$n \mid 3$ & $n-1 \mid 2 \Rightarrow n \equiv 3 \pmod 6$.

$n \mid 5$ & $n-1 \mid 4 \Rightarrow n \equiv 4 \pmod{20}$

Exercise 9.3. *Find a Carmichael numbers in the interval* $(1700, 1800)$.

consider $1729 = 7 \times 13 \times 19$.

$1729 - 1 = 1728$. $1728 = 6 \times 288 = 12 \times 144 = 18 \times 96$. by Prop. 9.4. it's a Carmichael number.

Exercise 9.4. *Show that every strong pseudoprime to base a is a pseudoprime to base a*

Pf: consider strong pseudoprime number $n = 2^s d + 1$. s.t. $a^d \equiv 1 \pmod n$. and $a^{2^r d} \equiv -1 \pmod n$. for all $0 \le r < s$

apply Fermat test for n. $a^{n-1} \equiv a^{2^s d} \equiv (a^{2^{s-1} d})^2 \equiv (-1)^2 \equiv 1 \pmod n$. thus it passes the Fermat's test to base a.

Exercise 9.5. *Determine if* 3281 *is a pseudoprime to base* 3*?*

Check: Find that $3281 = 17 \times 193$ - composite number.

Apply Fermat's test. (Note that $3^8 = 6561 = 3281 \times 2 - 1$).

$3^{3280} \equiv (-1)^{410} \equiv 1 \pmod{3281}$. → pass. it's a pseudoprime. to base 3.

HW 7. Week 8.

Exercise 11.1. *Prove the formulas for g_3, g_6, g_9, g_{12} from the above example.*

2022111221

Pf: $\alpha^3 = t^3$

$\alpha^6 = t^3(t+1) = t^3 + t^2$

$\alpha^9 = (t+1)^3 t = t^3 + t$

$\alpha^{12} = (t+1)^3 = t^3 + t^2 + t + 1$

$\alpha^{18} = (\alpha^9)^2 = (t^3+t)^2 = t^6 + t^2 = t^3$

$\alpha^{24} = \alpha^{18} \cdot \alpha^6 = t^3(t^3+t^2) = t^3 + t^2 + t^5 = t^3 + t$

$\alpha^{27} = \alpha^{18} \cdot \alpha^9 = t^6 + t^4 = t^3 + t^2 + t + 1$

$\alpha^{36} = (\alpha^{18})^2 = (t^3)^2 = t^3 + t^2$

$\alpha^{48} = (\alpha^{24})^2 = t^6 + t^2 = t^3$.

check $g_i(\alpha^i) = 0$

$i=3$: $\alpha^{12} + \alpha^9 + \alpha^6 + \alpha^3 + \bar{1} = 4t^3 + 2t^2 + 2t + \bar{1} + \bar{1} = \bar{0}$

$i=6$: $\alpha^{24} + \alpha^{18} + \alpha^{12} + \alpha^6 + \bar{1} = 4t^3 + 2t^2 + 2t + \bar{1} + \bar{1} = \bar{0}$

$i=9$ $\alpha^{36} + \alpha^{27} + \alpha^{18} + \alpha^9 + \bar{1} = \bar{0}$

$i=12$ $\alpha^{48} + \alpha^{36} + \alpha^{24} + \alpha^{12} + \bar{1} = \bar{0}$

it remains to check no quadratic polynomial over $\mathbb{Z}/2\mathbb{Z}$ has $\alpha^3, \alpha^6, \alpha^9, \alpha^{12}$ as it's root.

denote the polynomial be $h(t) = c_2 t^2 + ct + c_0$.

$\bar{0} = c_2\alpha^6 + c_1\alpha^2 + c_0$ $\quad t^6+t^3+t^2+t+\bar{1} \mid (c_2+c_1)t^3 + c_2t^2 + c_0 = \bar{0} \iff c_0 = c_1 = c_2 = 0$

similarly. for α^6 $\quad t^6+t^3+t^2+t+\bar{1} \mid (c_1+c_2)t^3 + (c_1+c_2)t^2 + c_2t + c_0 + c_2 = \bar{0} \iff c_0 = c_1 = c_2 = 0$

for α^9 $\quad t^6+t^3+t^2+t+\bar{1} \mid (c_1+c_2)t^3 + c_1t + c_0 \iff c_0 = c_1 = c_2 = 0$

for α^{12} $\quad t^6+t^3+t^2+t+\bar{1} \mid (c_1+c_2)t^3 + c_1t^2 + (c_1+c_2)t + c_1 + c_0 \iff c_0 = c_1 = c_2 = 0$

Exercise 11.2. *Consider the BCH code from the above example for $d = 5$.*

i) *Are* 1101000010000001, 1000000100011011 *its codewords?*

ii) *The received word* 1011000000001010 *has errors in two bits. Find the original codeword.*

i) 15 digit $\Rightarrow$ $x^{14} + x^7 + x^3 + x + \bar{1}$ and $x^{14} + x^{12} + x^{11} + x^7 + \bar{1}$

it suffices to check $x^8 + x^7 + x^6 + x^4 + \bar{1} \mid x^{14} + x^7 + x^3 + x + \bar{1}$ and $x^{14} + x^{13} + x^{11} + x^7 + \bar{1}$

$$
\begin{array}{r|l}
 & x^6 + x^5 + x^3 \\
\hline
x^8+x^7+x^6+x^4+\bar{1} & x^{14} + \qquad x^7 + x^3 + x + \bar{1} \\
 & x^{14} + x^{13} + x^{12} + x^{10} + x^6 \\
\hline
 & x^{13} + x^{12} + x^{10} + x^7 + x^6 \\
 & x^{13} + x^{12} + x^{11} + x^9 + x^5 \\
\hline
 & x^{11} + x^{10} + x^9 + x^7 + x^6 + x^5 + x^3 \\
 & x^{11} + x^{10} + x^9 + x^7 \qquad + x^3 \\
\hline
 & x^6 + x^5 + x + \bar{1} \neq 0.
\end{array}
$$

$$
\begin{array}{r|l}
 & x^6 + x^4 + \bar{1} \\
\hline
x^8+x^7+x^6+x^4+\bar{1} & x^{14} + x^{13} + x^{11} + x^7 + \bar{1} \\
 & x^{14} + x^{13} + x^{12} + x^{10} + x^6 \\
\hline
 & x^{12} + x^{11} + x^{10} + x^7 + x^6 \\
 & x^{12} + x^{10} + x^{10} + x^8 + x^4 \\
\hline
 & x^8 + x^7 + x^6 + x^4 + \bar{1} \\
 & x^8 + x^7 + x^6 + x^4 + \bar{1} \\
\hline
 & \bar{0}
\end{array}
$$

1st one. not BCH code. 2nd one is BCH code

ii). find the remainder of the word's polynomial divide by $x^8 + x^7 + x^6 + x^4 + \bar{1}$

$$
\begin{array}{r|l}
 & x^5 + x^4 + x^3 + \bar{1} \\
\hline
x^8+x^7+x^6+x^4+\bar{1} & x^{13} + x^{11} + x^3 + x^2 + \bar{1} \\
 & x^{13} + x^{12} + x^{11} + x^9 + x^5 \\
\hline
 & x^{12} + x^9 + x^5 + x^3 \\
 & x^{12} + x^{11} + x^{10} + x^8 + x^4 \\
\hline
 & x^{11} + x^{10} + x^9 + x^8 + x^5 + x^4 + x^3 \\
 & x^{11} + x^{10} + x^9 + x^7 + x^3 \\
\hline
 & x^8 + x^7 + x^5 + x^4 + x^2 + \bar{1} \\
 & x^8 + x^7 + x^6 + x^4 + \bar{1} \\
\hline
 & x^6 + x^5 + x^2
\end{array}
$$

(maybe 3 error ?). "$\rightarrow$" 4th. 6th. 7th. reverse

1010011000010010.

Exercise 11.3. *Let $p = 2, n = 5$ and $K = \mathbb{Z}/2\mathbb{Z}[t]/(t^5 + t^2 + \bar{1})$. Calculate the generator polynomials for BCH codes corresponding to $d = 2, \ldots 8$.*

Sol: $|K^*| = 2^5 - 1 = 31$.

primitive root: t.

$\alpha = t$	$\alpha^3 = t^3$	$\alpha^5 = t^2 + \bar{1}$	$\alpha^6 = t^3 + t$	$\alpha^7 = t^4 + t^2$
$\alpha^2 = t^2$	$\alpha^6 = t^3 + t$	$\alpha^{10} = t^4 + \bar{1}$	$\alpha^{12} = t^3 + t^2 + t$	$\alpha^{14} = t^4 + t^3 + t^2 + \bar{1}$
$\alpha^4 = t^4$	$\alpha^9 = t^4 + t^3 + t$	$\alpha^{15} = t^4 + t^3 + t^2 + t + \bar{1}$	$\alpha^{18} = t + 1$	$\alpha^{21} = t^4 + t^3$
$\alpha^8 = t^3 + t^2 + \bar{1}$	$\alpha^{12} = t^3 + t^2 + t$	$\alpha^{20} = t^3 + t^2$	$\alpha^{24} = t^4 + t^3 + t^2 + t$	$\alpha^{28} = t^4 + t^2 + t$.
$\alpha^{16} = t^4 + t^3 + t + \bar{1}$	$\alpha^{15} = t^4 + t^3 + t^2 + t + \bar{1}$	$\alpha^{25} = t^4 + t^3 + \bar{1}$	$\alpha^{30} = t^4 + t$	$\alpha^{35} = \alpha^4 = t^4$

for minimal polynomial. (choose some (in 1 column) term from the table above to eliminate the coefficient for each power).

$g_1 = g_2 = g_4 = t^5 + t^2 + \bar{1}$

$g_3 = g_6 = t^5 + t^4 + t^3 + t^2 + \bar{1}$

$g_5 = t^5 + t^4 + t^2 + t + \bar{1}$

$g_7 = t^5 + t^3 + t^2 + t + \bar{1}$

for every d. we need to find the minimal polynomial 's lcm less than d.

$d = 2, 3$. $g = \text{lcm}(g_1) = t^5 + t^2 + \bar{1}$.

$d = 4, 5$ $g = \text{lcm}(g_1, g_3) = t^{10} + t^9 + t^8 + t^6 + t^5 + t^3 + \bar{1}$

$d = 6, 7$ $g = \text{lcm}(g_1, g_3, g_5) = t^{15} + t^{12} + t^9 + t^8 + t^7 + t^5 + t^3 + t^2 + t + \bar{1}$

$d = 8$ $g = \text{lcm}(g_1, g_3, g_5, g_7) = t^{20} + t^{18} + t^{16} + t^9 + t^7 + t^6 + t^4 + t^2 + \bar{1}$

$\downarrow$ $t^5 + t^4 + t^2 + t + \bar{1}$

$\downarrow$ $t^5 + t^3 + t^2 + t + \bar{1}$