

homework 4

$$1. \begin{cases} x \equiv a_1 \pmod{11} \\ x \equiv a_2 \pmod{13} \end{cases}$$

$x \equiv a_3 \pmod{17}$ since 11, 13, 17, 19 are pairwise
 $x \equiv a_4 \pmod{19}$ relatively prime

so let $b_1 = [a_1]_{11}$, $b_2 = [a_2]_{13}$, $b_3 = [a_3]_{17}$, $b_4 = [a_4]_{19}$
 $n_1 = 11$, $n_2 = 13$, $n_3 = 17$, $n_4 = 19$

$$N = n_1 \cdot n_2 \cdot n_3 \cdot n_4 = 46189$$

$$N_1 = \frac{N}{n_1} = 4199, \quad N_2 = \frac{N}{n_2} = 3553$$

$$N_3 = \frac{N}{n_3} = 2717, \quad N_4 = \frac{N}{n_4} = 2431 \quad \text{and } 11, 13$$

since $\gcd(1, 11) = 1 \mid \cancel{a_1}$, $\gcd(1, 13) = 1 \mid \cancel{[a_2]_{13}}$
 $\gcd(1, 17) = 1 \mid a_3$, $\gcd(1, 19) = 1 \mid a_4$ a_1, a_2
Pairwise
relatively
prime

so are the congruence equations have solutions

and the linear congruence equations

is equivalent to

$$\begin{cases} x \equiv [a_1]_{11} \pmod{11} \\ x \equiv [a_2]_{13} \pmod{13} \\ x \equiv [a_3]_{17} \pmod{17} \\ x \equiv [a_4]_{19} \pmod{19} \end{cases} \Rightarrow \begin{cases} x \equiv b_1 \pmod{11} \\ x \equiv b_2 \pmod{13} \\ x \equiv b_3 \pmod{17} \\ x \equiv b_4 \pmod{19} \end{cases}$$

according to CRT

let $s_1 N_1 \equiv 1 \pmod{11}$, $s_2 N_2 \equiv 1 \pmod{13}$

$s_3 N_3 \equiv 1 \pmod{17}$, $s_4 N_4 \equiv 1 \pmod{19}$

since 11, 13, 17, 19 are all primes
 according to Fermat's little theorem

we know that if P is prime

then $\forall a \in \{[1]_P, [2]_P, \dots, [P-1]_P\}$

$$a^{P-1} \equiv 1 \pmod{P}$$

$$\text{so } a \cdot (a^{P-2}) \equiv 1$$

so $[a^{P-2}]_P$ is the inverse of a
 in the module of P

Since s_1, s_2, s_3, s_4 is the inverse of n_1, n_2, n_3, n_4

$$\text{so } s_1 \equiv ([n_1]_{11})^{11-2} \equiv 8^9 \equiv 7 \pmod{11}$$

$$s_2 \equiv ([n_2]_{13})^{13-2} \equiv 4^{11} \equiv 10 \pmod{13}$$

$$s_3 \equiv ([n_3]_{17})^{17-2} \equiv 14^{15} \equiv 11 \pmod{17}$$

$$s_4 \equiv ([n_4]_{19})^{19-2} \equiv 18^{17} \equiv 18 \pmod{19}$$

$$\text{let } s_1 = 7, s_2 = 10, s_3 = 11, s_4 = 18$$

$$\text{so let } b = b_1(s_1, n_1) + b_2(s_2, n_2) + b_3(s_3, n_3) + b_4(s_4, n_4)$$

$$\text{since } x \equiv b \pmod{N}$$

$$\text{so } x = [a_1]_N [s_1]_N [n_1]_N + [a_2]_N [s_2]_N [n_2]_N$$

$$+ [a_3]_N [s_3]_N [n_3]_N + [a_4]_N [s_4]_N [n_4]_N$$

$$x = [a_1]_N [7 \times 4199]_N + [a_2]_N [10 \times 3553]_N$$

$$+ [a_3]_N [11 \times 2717]_N + [a_4]_N [18 \times 2431]_N$$

$$\text{so } x = [29393a_1 + 35530a_2 + 29887a_3 + 43758a_4]_{46189}$$

above all, $x = 29393a_1 + 35530a_2 + 29887a_3 + 43758a_4 + 46189n, n \in \mathbb{Z}$ are all integer solutions

2. let $x = m^3$

$$\text{so } \begin{cases} x \equiv c_1 \pmod{N_1} \\ x \equiv c_2 \pmod{N_2} \\ x \equiv c_3 \pmod{N_3} \end{cases}$$

Since N_1, N_2, N_3 are pairwise relative prime

so we can use CRT to solve it

$$\text{let } N = N_1 N_2 N_3, n_1 = N_2 N_3, n_2 = N_1 N_3, n_3 = N_1 N_2$$

$$\gcd(n_1, N_1) = 1, \gcd(n_2, N_2) = 1, \gcd(n_3, N_3) = 1$$

~~from~~ so there must exist $s_1, s_2, s_3 \in \mathbb{Z}$

$$\text{s.t. } s_1 n_1 \equiv 1 \pmod{N_1}, s_2 n_2 \equiv 1 \pmod{N_2}, s_3 n_3 \equiv 1 \pmod{N_3}$$

and we can compute s_1, s_2, s_3 through EEA.

~~$$\text{so } x \equiv c_1(s_1 n_1) + c_2(s_2 n_2) + c_3(s_3 n_3) \pmod{N}$$~~

~~$$\text{so } x \equiv c_1(s_1 n_1) + c_2(s_2 n_2) + c_3(s_3 n_3) \pmod{N}$$~~

let x_1 be the smallest positive integer

among all the solutions

$$\text{so } 0 \leq x_1 < N \text{ which means } 0 \leq x_1 < N_1 N_2 N_3$$

$$\text{since } 0 \leq m < N_i, i=1,2,3$$

$$\text{so } 0 \leq m^3 < N_1 N_2 N_3 \Rightarrow 0 \leq x < N_1 N_2 N_3$$

so x_1 and m^3 are in the same range

$$\text{so } 0 \leq |x_1 - m^3| < N_1 N_2 N_3 \quad ①$$

$$\text{since } x_1 \equiv x \pmod{N}, x = m^3 \text{ so } x_1 \equiv m^3 \pmod{N}$$

$$\text{so } x_1 - m^3 = k N_1 N_2 N_3, k \in \mathbb{Z} \text{ from } ① \text{ we know that}$$

$$\text{so } m = \sqrt[3]{x_1} \text{ ; } k \text{ must equal to } 0 \text{ so } x_1 = m^3$$

above all, ~~we~~ can decide the value of m .

Eve

$$3. G = \{x : x \in \mathbb{R}, x > 1\}, x * y = xy - x - y + 2$$

<1> closure $\forall a, b \in G$ which means $a > 1, b > 1$

$$\text{So } a * b = ab - a - b + 2 = (a-1)(b-1) + 1 > 1$$

$$\text{So } a * b \in G$$

<2> associative $\forall a, b, c \in G$

$$a * (b * c) = a * (bc - b - c + 2) = a(bc - b - c + 2)$$

$$- a - (bc - b - c + 2) + 2 = abc - ab - bc - ac + a + b + c$$

$$(a * b) * c = (ab - a - b + 2) * c$$

$$= (ab - a - b + 2)c - (ab - a - b + 2) - c + 2$$

$$= abc - ab - bc - ac + a + b + c$$

$$\text{So } a * (b * c) = (a * b) * c \quad \square$$

<3> identity element $\exists e$

~~let~~ let $e = 2, e \in G$

$$a * e = ae - a - e + 2 = 2a - a - 2 + 2 = a$$

$$e * a = ea - e - a + 2 = 2a - 2 - a + 2 = a$$

$$\text{So } a * e = e * a = a$$

NO _____

DATE _____

$\langle 4 \rangle$ inverse. $\forall a \in G$

$$\text{let } b = \frac{a}{a-1}$$

$$\text{since } a > 1 \quad \text{so } b = \frac{a}{a-1} = \frac{a-1+1}{a-1} = 1 + \frac{1}{a-1} > 1$$

$$\text{so } b \in G$$

$$\begin{aligned} a * b &= ab - a - b + 2 = a \cdot \frac{a}{a-1} - a - \frac{a}{a-1} + 2 \\ &= \frac{a^2 - a^2 + a - a}{a-1} + 2 = 2 = e. \end{aligned}$$

$$\begin{aligned} b * a &= ba - b - a + 2 = \frac{a}{a-1}a - \frac{a}{a-1} - a + 2 \\ &= \frac{a^2 - a - a^2 + a}{a-1} + 2 = 2 = e \end{aligned}$$

$$\text{so } \forall a \in G, \exists b = \frac{a}{a-1} \in G$$

$$\text{s.t. } a * b = b * a = e \quad \square$$

\Leftrightarrow above all $(G, *)$ is a group

$\langle 5 \rangle$ commutative

$$\forall a, b \in G$$

$$a * b = ab - a - b + 2 = ba - b - a + 2 = b * a$$

$$\text{so } a * b = b * a$$

so $(G, *)$ is an Abelian group

multiplicative
✓

4. (G, \cdot) is an Abelian group

~~from~~ $\text{ord}(G) = m \quad |G| = m$

from Euler's Theorem

we know that $\forall a \in G$

$$a^{|G|} = 1$$

$$\text{so } a^m = 1$$

from the definition $\text{ord}(a) \leq m$

c.i) if $\text{ord}(a) = m$ then $m \mid m$

$$\text{so } \text{ord}(a) \mid m \quad \square$$

c.ii) if $\text{ord}(a) = l < m$

then from division algorithm

there exist uniquely $q, r \in \mathbb{Z}$ s.t. ~~$0 < r < l$~~ , $0 \leq r < l$

the $m = lq + r$ since $m > 0$, so $q \geq 0$

then since $a^m = 1$

$$\text{so } a^{lq+r} = 1 \quad \text{the } (a^l)^q \cdot a^r = 1$$

since $\text{ord}(a) = l$ so $a^l = 1$

$$\text{so } a^r \cdot 1^q = 1$$

$$\text{so } a^r = 1$$

<1> if $\text{ord}(a) = l \mid m$, then $r=0$, is correct

<2> if $\text{ord}(a) = l \nmid m$, then $0 < r < l$

since $0 < r < l$ so the order of a should be r instead of l
so it's not correct so $\text{ord}(a) \neq l$

so above all $\text{ord}(a) \mid m$