NO

DATE

homework 4

1. $\begin{cases} x \equiv a_1 \pmod{11} \\ x \equiv a_2 \pmod{13} \\ x \equiv a_3 \pmod{17} \\ x \equiv a_4 \pmod{19} \end{cases}$ since 11, 13, 17, 19 are pairwise relatively prime

So let $b_1 = [a_1]_{11}$, $b_2 = [a_2]_{13}$, $b_3 = [a_3]_{17}$, $b_4 = [a_4]_{19}$

$n_1 = 11$, $n_2 = 13$, $n_3 = 17$, $n_4 = 19$

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

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

$N_3 = \frac{N}{n_3} = 2717$, $N_4 = \frac{N}{n_4} = 2431$

since $\gcd(1, 11) = 1 \mid a_1$, $\gcd(1, 13) = 1 \mid a_2$, and 11, 13, 17, 19 are pairwise relatively prime

$\gcd(1, 17) = 1 \mid a_3$, $\gcd(1, 19) = 1 \mid a_4$

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 $S_1 N_1 \equiv 1 \pmod{11}$, $S_2 N_2 \equiv 1 \pmod{13}$

$S_3 N_3 \equiv 1 \pmod{17}$, $S_4 N_4 \equiv 1 \pmod{19}$

NO

DATE

since 11, 13, 17, 19 are all primes
according to Fermat's little theorem
we know that if P is prime
then $\forall a \in \{[1]_p, [2]_p, \ldots [p-1]_p\}$
$a^{p-1} \equiv 1 \pmod p$
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

so $s_1 \equiv ([N_1]_{11})^{11-2} \equiv 8^9 \equiv 7 \pmod{11}$
$s_2 \equiv ([N_2]_{13})^{13-2} \equiv 4^{11} \equiv 10 \pmod{13}$
$s_3 \equiv ([N_3]_{17})^{17-2} \equiv 14^{15} \equiv 11 \pmod{17}$
$s_4 \equiv ([N_4]_{19})^{19-2} \equiv 18^{17} \equiv 18 \pmod{19}$

let $s_1 = 7, s_2 = 10, s_3 = 11, s_4 = 18$

so let $b = [b_1(s_1 N_1) + b_2(s_2 N_2) + b_3(s_3 N_3) + b_4(s_4 N_4)]$
since $x \equiv b \pmod N$
so $x = [a_1]_N [s_1]_N [N_1]_N + [a_2]_N [s_2]_N [N_2]_N$
$+ [a_3]_N [s_3]_N [N_3]_N + [a_4]_N [s_4]_N [N_4]_N$

$x = [a_1]_N [7 \times 4199]_N + [a_2]_N [10 \times 3553]_N$
$+ [a_3]_N [11 \times 2717]_N + [a_4]_N [18 \times 2431]_N$

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

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

NO

DATE

2. let $x = m^3$

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

let $N = N_1N_2N_3$, $n_1 = N_2N_3$, $n_2 = N_1N_3$, $n_3 = N_1N_2$

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

so their must exist $s_1, s_2, s_3 \in \mathbb{Z}$

s.t. $s_1n_1 \equiv 1 \pmod{N_1}$, $s_2n_2 \equiv 1 \pmod{N_2}$, $s_3n_3 \equiv 1 \pmod{N_3}$

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

~~so $x \equiv c_1(s_1N_1) + c_2(s_2N_2) + c_3(s_3N_3) \pmod{N}$~~

so $x \equiv c_1(s_1n_1) + c_2(s_2n_2) + c_3(s_3n_3) \pmod{N}$

let x_1 be the smallest positive interger among all the solutions

so $0 \le x_1 < N$ which means $0 \le x_1 < N_1N_2N_3$

since $0 \le m < N_i$, $i = 1, 2, 3$

so $0 \le m^3 < N_1N_2N_3 \Rightarrow 0 \le x < N_1N_2N_3$

so x_1 and m^3 are in the same range

so $0 \le |x_1 - m^3| < N_1N_2N_3$ ①

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

so $x_1 - m^3 = kN_1N_2N_3$, $k \in \mathbb{Z}$ from ① we know that k must equal to 0 so $x_1 = m^3$

so $m = \sqrt[3]{x_1}$

above all, Eve can decide the value of m.

NO

DATE

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

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

So $a*b=ab-a-b+2=(a-1)(b-1)+1>1$

So $a*b\in G$

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

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

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

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

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

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

So $a*(b*c)=(a*b)*c$ □

<3> identity element $\exists e$

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

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

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

So $a*e=e*a=a$

NO

DATE

<4> inverse. $\forall a \in G$

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

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

so $b \in G$

$a * b = ab - a - b + 2 = a \cdot \frac{a}{a-1} - a - \frac{a}{a-1} + 2$

$= \frac{a^2 - a^2 + a - a}{a-1} + 2 = 2 = e.$

$b * a = ba - b - a + 2 = \frac{a}{a-1} - a - \frac{a}{a-1} - a + 2$

$= \frac{a^2 - a - a^2 + a}{a-1} + 2 = 2 = e$

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

s.t. $a * b = b * a = e$ □

⇐ above all $(G, *)$ is a group

<5> commutative

$\forall a, b \in G$

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

so $a * b = b * a$

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

NO

DATE

multiplicative

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

~~from~~ $o(G) = m$ $|G| = m$

from Euler's Theorem

we know that $\forall a \in G$

$a^{|G|} = 1$

so $a^m = 1$

from the defination $o(a) \leq m$

(i) if $o(a) = m$ then $m | m$

so $o(a) | m$ □

(ii) if $o(a) = l < m$

then from division algorithm

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

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

then since $a^m = 1$

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

since $o(a) = l$ so $a^l = 1$

so $a^r \cdot 1^q = 1$

so $a^r = 1$

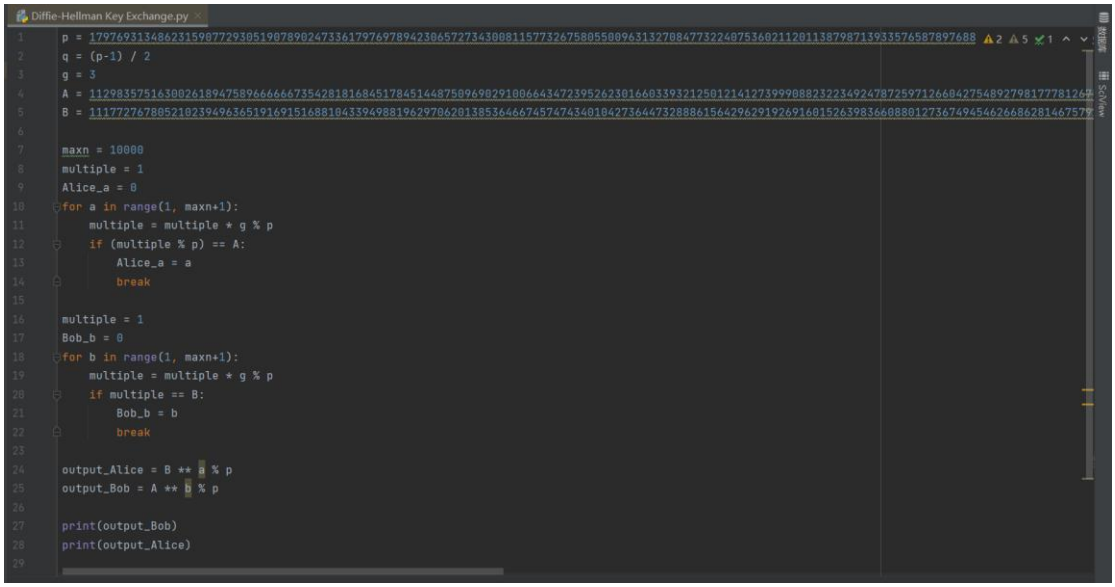
<1> if $o(a) = l | m$, then $r = 0$, is correct

<2> if $o(a) = l \nmid m$, then $0 < r < l$

since $0 < r < l$ so the order of a should be r instead is of l

so it's not correct ~~so $o(a) \neq l$~~

So above all $o(a) | m$




```
p = 179769313486231590772930519078902473361797697894230657273430081157732675805500963132708477322407536021120113879871393357658789768814416622492847430639474124377767893424865485276302219601246094119453082952085005768838150682342462881473913110540827237163350510684586298239947245938479716304835356329624227998859
q = (p-1) / 2
g = 3
A = 112983575163002618947589666666735428181684517845144875096902910066434723952623016603393212501214127399908823223492478725971266042754892798177781267512821607470545283059472689034731313027619864228688466438258327552045437590203790635506728603774799021127049872571983254506993921153718739796769296097404717448108
B = 111772767805210239496365191691516881043394988196297062013853646674574743401042736447328886156429629192691601526398366088012736749454626686281467579205675084461989494513294624066074137247913037330040487275346913253345733429767781900977102687185378411660147190296412313303321533586102552123457499563789255321369

maxn = 10000
multiple = 1
Alice_a = 0
for a in range(1, maxn+1):
    multiple = multiple * g % p
    if (multiple % p) == A:
        Alice_a = a
        break

multiple = 1
Bob_b = 0
```

```
for b in range(1, maxn+1):
        multiple = multiple * g % p
        if multiple == B:
                Bob_b = b
                break

output_Alice = B ** a % p
output_Bob = A ** b % p

print(output_Bob)
print(output_Alice)

# k = output_Alice = output_Bob =
1082811278345346238104170780205614986659639207224390394098745967277926067531952266309908038877090398254625052499242035020020762432742061230017062080266530290575004577768434812582748436500759071863837318793688996730932472265529499222581541091410507221072504595310501935245754077299550897831569910724739835012 8
```