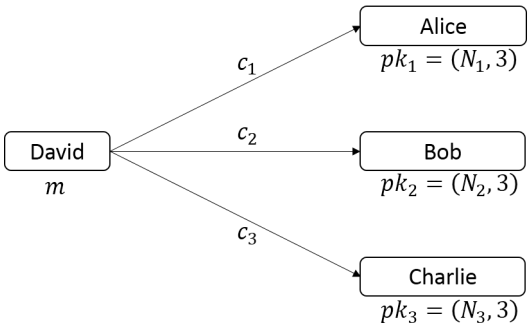
Discrete Mathematics: Homework 4

(Deadline: 8:00am, March 18, 2022)

1. (20 points) Let a_1, a_2, a_3, a_4 be arbitrary integers. Find ALL integer solutions of the following equation system.

$$\begin{cases} x \equiv a_1 (\text{mod } 11); \\ x \equiv a_2 (\text{mod } 13); \\ x \equiv a_3 (\text{mod } 17); \\ x \equiv a_4 (\text{mod } 19). \end{cases}$$

2. (20 points) See the following figure. The RSA public keys of Alice, Bob and Charlie are $pk_1 = (N_1, 3), pk_2 = (N_2, 3)$ and $pk_3 = (N_3, 3)$, respectively. David wants to send a private message m to Alice, Bob and Charlie, where m is an integer and $0 < m < N_i$ for $i = 1, 2, 3$. In order to keep m secret from an eavesdropper Eve, David encrypts m as $c_1 = m^3 \bmod N_1$, $c_2 = m^3 \bmod N_2$ and $c_3 = m^3 \bmod N_3$; and then sends c_1 to Alice, c_2 to Bob and c_3 to Charlie.



Suppose that N_1, N_2, N_3 are pairwise relatively prime. Show that with the knowledge of all public keys and all ciphertexts, Eve can decide the value of m.

3. (20 points) Let $G = \{x : x \in \mathbb{R}, x > 1\}$. Define $x \star y = xy - x - y + 2$ for all $x, y \in \mathbb{R}$. Show that $(G, \star)$ is an Abelian group.

4. (20 points) Let $(G, \cdot)$ be a multiplicative (Abelian) group of order m. Show that $o(a)|m$ for any $a \in G$, i.e., the order of any group element must be a divisor of the group's order.

5. (20 points) Let $G = \langle g \rangle$ be a subgroup of $\mathbb{Z}_p^*$ of order q, where

```
p=17976931348623159077293051907890247336179769789423065727343008115773267580550096313270847732240753602112011387987139335765878976881441662249284743063947412437776789342486548527630221960124609411945308295208500576883815068234246288147391311054082723716335051068458629823994724593847971630483535632962422799885 9,
```

$q = (p-1)/2$ and $g = 3$. Suppose that in a Diffie-Hellman key exchange protocol Alice and Bob exchanged the following information $(q, G, g; A, B)$, where

```
A=112983575163002618947589666666735428181684517845144875096902910066434723952623016603393212501214127399908823223492478725971266042754892798177781267512821607470545283059472689034731313027619864228688466438258327552045437590203790635506728603774799021127049872571983254506993921153718739796769296097404717448108;

B=111772767805210239496365191691516881043394988196297062013853646674574743401042736447328886156429629192691601526398366088012736749454626686281467579205675084461989494513294624066074137247913037330040487275346913253345733429767781900977102687185378411660147190296412313303321533586102552123457499563789255321369.
```

In particular, $\log_g A, \log_g B \leq 10^4$. Find the output of Alice and Bob.