Name:

COL202: Quiz-2
Maximum marks: 40 Kerberos id:

Instructions.

1. For each problem, you will receive 10% marks for leaving it blank. However, there will be penalty for submitting bogus proofs.

2. Please write your proofs clearly (marks will be deducted for skipping steps, not mentioning which PMI you are using, etc).

3. At the end of this paper, you will find the list of relevant theorems and properties proven in class/tutorials. In case you need to assume anything else, please explicitly state what you are assuming.

Question 1: Some More Properties of $\mathbb{Z}_p$ (20 marks). We say that a prime p is a *nice* prime if $p = 2q + 1$, where q is also prime. In this problem, we will study some properties of $\mathbb{Z}_p$ when p is a *nice* prime.

For any element a in $\mathbb{Z}_p \setminus \{0\}$, let $\text{ord}(a)$ (called the *order* of a) denote the smallest natural number such that $\exp_p(a, \text{ord}(a)) = 1$. In this problem, we will show that many elements of $\mathbb{Z}_p$ have order q. Elements with prime order are very useful in cryptography.

For instance, $p = 11$ is a nice prime, the orders of the elements of $\mathbb{Z}_p \setminus \{0\}$ are given in Table 1. Note that four elements $(2, 6, 7$ and $8)$ have order 10, and four elements $(3, 4, 5$ and $9)$ have order 5.

Part 1. Prove that at least one element has order q. (6 marks)

Part 2. Using Part 1 or otherwise, prove that at least $q - 1$ elements in $\mathbb{Z}_p \setminus \{0\}$ have order q. (9 marks)

Part 3. Finally, prove that exactly $q - 1$ elements in $\mathbb{Z}_p \setminus \{0\}$ have order q. (5 marks)

a	Powers of a modulo $p = 11$	$\text{ord}(a)$
1	1 1 1 1 1 1 1 1 1 1 1	1
2	1 2 4 8 5 10 9 7 3 6 1	10
3	1 3 9 5 4 1 3 9 5 4 1	5
4	1 4 5 9 3 1 4 5 9 3 1	5
5	1 5 3 4 9 1 5 3 4 9 1	5
6	1 6 3 7 9 10 5 8 4 2 1	10
7	1 7 5 2 3 10 4 6 9 8 1	10
8	1 8 9 6 4 10 3 2 5 7 1	10
9	1 9 4 3 5 1 9 4 3 5 1	5
10	1 10 1 10 1 10 1 10 1 10 1	2

Table 1: In this table, the powers of a are listed modulo p. The i^{th} element in the list is $\exp_p(a, i - 1)$.

Question 2 (20 marks). The Fibonacci sequence is defined as follows:

$$F_n = \begin{cases} 1 \text{ if } n = 1 \\ 1 \text{ if } n = 2 \\ F_{n-1} + F_{n-2} \text{ if } n > 2 \end{cases}$$

The first few elements of the Fibonacci sequence are as follows:

F_1	F_2	F_3	F_4	F_5	F_6	F_7	F_8	F_9	F_{10}	F_{11}	F_{12}	F_{13}	F_{14}	F_{15}
1	1	2	3	5	8	13	21	34	55	89	144	233	377	610

Prove that for all n, m, if n divides m, then F_n divides F_m.

[**Hint** : Look at the sequences $(F_1, F_2, \ldots, F_n)$ and $(F_{n+1}, F_{n+2}, \ldots, F_{2n})$. There is some similarity in these two sequences. Similarly, there is some similarity between $(F_1, F_2, \ldots, F_n)$ and $(F_{kn+1}, F_{kn+2}, \ldots, F_{(k+1)n})$ for all k. First show that for all n, F_n divides F_{2n}. Then, using induction, show that if F_n divides F_{kn}, then F_n also divides $F_{(k+1)n}$.]

[[**Additional Hints** : You can ask the instructor or TA Anish Banerjee for additional hints. There is a -5 penalty associated with the extra hint (penalty applicable only if you are able to solve the question).]]