Sp'16: MATH 2513–002 **Discrete Mathematics** **Noel Brady**

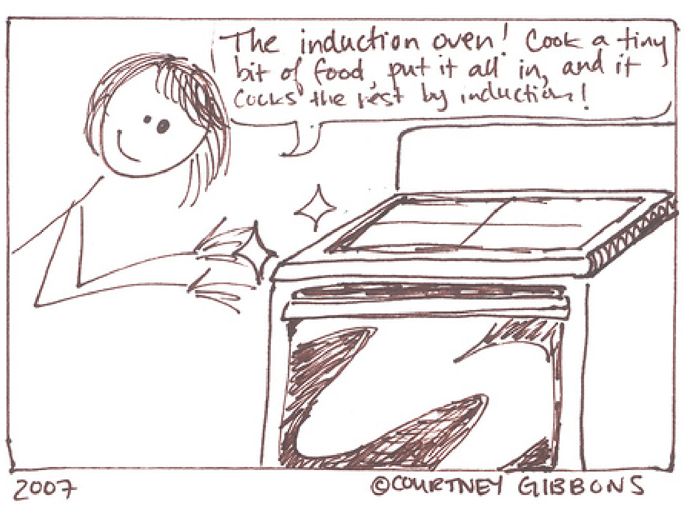
Friday 03/11/2016 Midterm II 50 mins

Name: ______________________ Student ID: ______________________

Instructions.

1. Attempt all questions.
2. Do not write on back of exam sheets. Extra paper is available if you need it.
3. Show all the steps of your work clearly.

Question	Points	Your Score
Q1	20	
Q2	20	
Q3	20	
Q4	20	
Q5	20	
TOTAL	100	



Miscellaney.

1. **Least Principle.** Every non-empty subset of $\mathbb{N}$ contains a least element.
2. **Theorem. (Division Algorithm)** Let $d \in \mathbb{N}$ and $a \in \mathbb{Z}$. Then there exists unique integers $q, r \in \mathbb{Z}$ such that
$$a = qd + r$$
where $0 \leq r < d$.
3. **Proposition [Euclidean Algorithm].** Let a and b be integers and b positive. By the Division Algorithm there are unique integers q, r so that
$$a = bq + r \qquad \text{and } 0 \leq r < b.$$
Then
$$\gcd(a, b) = \gcd(b, r).$$
4. **Proposition (Bezout's identity).** Let a, b be integers, not both zero. Then there exist integers l, m such that
$$\gcd(a, b) = la + mb.$$
5. **Corollary (Euclid's Lemma).** Let p, b, c be integers, and p a prime number. If $p \mid bc$ and $p \nmid b$, then $p \mid c$.
6. **Theorem (Fundamental Theorem of Arithmetic).** Every integer a greater than or equal to 2 can be expressed as a product of prime numbers. That is
$$a = p_1 \dots p_n$$
where the p_j are primes. This includes the special case of $n = 1$ and so a is prime.

Furthermore, this expression is unique if we require that the primes be listed in non-decreasing order.
$$p_1 \leq p_2 \leq \cdots \leq p_n.$$
7. **Theorem (Fermat's Little Theorem).** Let p be a prime number and let a be a nonzero element of $\mathbb{Z}_p$. Then
$$a^{p-1} \equiv 1 \mod p.$$

Q1]... [20 points] State the Principle of Induction.

Give a proof by induction of the following statement.

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6} \qquad \text{for all } n \in \mathbb{N}.$$

Q2]... [20 points] Give a proof of the following statement.
If a natural number n is not a perfect cube (that is n is not one of $1, 8, 27, 64, \ldots$), then its cube root $\sqrt[3]{n}$ is irrational.

Q3]...[20 points] Compute gcd(729, 354) and find integers c and d such that

$$729c + 354d \;=\; \gcd(729, 354).$$

Recall that the Fibonacci numbers are defined by $F_1 = 1 = F_2$ and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 3$. Give a proof of the following statement.

$$\gcd(F_n, F_{n-1}) \;=\; 1 \qquad\qquad \text{for all integers } n \geq 2.$$

Q4]. . . [20 points] You have access to a water faucet and two drinking glasses, one with capacity exactly 21oz and the other with capacity exactly 13oz. Is it possible to measure out exactly 1oz of water? Either describe a series of steps that ends up with 1oz, or prove that it is impossible.

You have access to a water faucet and two drinking glasses, one with capacity exactly 21oz and the other with capacity exactly 15oz. Is it possible to measure out exactly 1oz of water? Either describe a series of steps that ends up with 1oz, or prove that it is impossible.

Q5]... [20 points] Use modular exponentiation rules to compute the following powers in modular arithmetic.

1. $(23)^{50} \mod 17$

2. $(2016)^{2016} \mod 11$

3. $3^{124} \mod 77$

Let p, q, r be three distinct prime numbers. Guess a **positive** integer power m so that

$$a^m \equiv 1 \mod pqr \qquad \text{for every integer } a \text{ such that } \gcd(a, pqr) = 1.$$

Now prove that your guess is correct.