MAT310 Final, Spring 2005

Name:

Directions: Show your work! Answers without justification will likely result in few points. Your written work also allows me the option of giving you partial credit in the event of an incorrect final answer (but good reasoning). Indicate clearly your answer to each problem (e.g., put a box around it).
Note: you may of course use your calculators, but the use of the calculator without analysis will not result in many points. **Good luck!**

Today's Special: you **must** skip one of problems 3-9 (but not problems 1 or 2). Write "skip" on the problem from which I should avert my eyes....

Problem 1 Prove that if $2|u_n$, then $4|(u_{n+1}^2 - u_{n-1}^2)$; and similarly, if $3|u_n$, then $9|(u_{n+1}^3 - u_{n-1}^3)$.

Problem 2.

A (6 pts). I am your opponent in Fibonacci Nim. Assume that you start (choose first); that I've put 32 sticks out on the table to begin; and that I play a conservative strategy, always taking exactly 1 stick. Show the resulting sequence of moves, provided you play the winning strategy strictly.

B (2 pts). Is there any way for you to win, provided you start the game faced with a Fibonacci number of sticks, against an opponent who knows the winning strategy? Why or why not?

C (2 pts). On what theorem is the winning strategy of Fibonacci Nim based?

Problem 3. Short answer:

- State Fermat's Last Theorem; state Fermat's Little Theorem.

- Describe Pythagoras's contributions that earned Pythagorean triples their name.

- What is the Sieve of Eratosthenes, and what else did Eratosthenes do in the field of earth science?

- Describe one of Euler's contributions to number theory. What do you know of Euler?

Problem 4. More short answer:

- What does the Fundamental Theorem of Arithmetic assert?

- What do we mean by "a complete set of residues mod n"? Give an example set for $n = 7$, which includes the number 9.

- What does it mean to say that a number-theoretic function is multiplicative? How is this property useful?

- Solve, with reasons:

$$20! \equiv \_\_\_\_\_ (mod 19)$$
$$19! \equiv \_\_\_\_\_ (mod 19)$$
$$18! \equiv \_\_\_\_\_ (mod 19)$$
$$17! \equiv \_\_\_\_\_ (mod 19)$$

Problem 5. If $p \geq q \geq 5$, and p and q are both primes, prove that

$$24 \mid p^2 - q^2$$

Problem 6.
A (4pts). Use the division algorithm (in all its glory) to calculate the gcd of 2005 and 42.

B (4pts). Write the gcd as a linear combination of the numbers 2005 and 42.

C (2pts). State the lemma (or theorem) that we are relying on to deduce the gcd from the calculations of the division algorithm.

Problem 7. The Pythagoreans believed that the world was built on whole numbers, so they were dismayed to learn that $\sqrt{2}$ was irrational (and their philosophy was absolutely shattered). Prove (by contradiction) that $\sqrt{p}$ is irrational for all primes p.

Problem 8. (A number theorist's idea of an applied problem:)
A band of seventeen roofers found a treasure trove of identical gold coins in the barn they were working on, and tried to divvy it up evenly; but they found that there were 15 coins left over, and so they brawled. In the melee, four roofers fell to their deaths from the barn roof. The 13 roofers remaining tried again, but again found a remainder of 11 coins. Rather than try to come to compromise, they brawled again, and three more roofers fell to their deaths. The roofers remaining tried once again, but found that 3 coins remained. Rather than brawl further, the roofers used the three coins to pay a priest to say masses for their dead friends, and made their getaways.

The number of coins in the barn was the smallest possible that satisfies the conditions above. How many were there?

Problem 9. (A number theorist's **real** applied problem!)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- In the use of Hill's cipher, why is the system of equations

$$C_1 \equiv 2P_1 + 3P_2 \pmod{26}$$
$$C_2 \equiv \ P_1 + 9P_2 \pmod{26}$$

  an acceptible system to use? Use it to encode the phrase "THINK IT OVER", using the standard alphabetic conversion (A=00, Z=25). Don't attempt to encrypt spaces, and pad with Xs as necessary.

- Use the RSA algorithm to encode the same message ("THINK IT OVER") letter by letter, using the primes $p = 7$ and $q = 19$, and take $k = 23$. Don't attempt to encrypt spaces.

- Compute the value of j that you will use to decypher messages using the RSA algorithm, with the values of p, q, and k above.

- Use the RSA method as configured above to decode the following message (coded letter by letter): 62 105 105 110 121 20 32 117.