

Number Theory
McGill 189-346/377B
Final Exam

Due at 4 p.m. on Friday, April 19th, 2002

Instructions: Solve as many of these problems as possible. Each of the ten questions is worth 10 points. However: **students in 189-346**, your total score will be graded out of **80**, so it is theoretically possible to score 100/80; **students in 189-377**, your total score will be graded out of **90**, so it is theoretically possible to score 100/90.

You are permitted to use the following resources: the required text for the course (Davenport, *The Higher Arithmetic*), your notes, your homework, and all handouts (including problem sets, the homework solutions, and the excerpt from Cox's book). You may also use a *non-programmable* calculator (or a programmable calculator, provided that you do not use any of the programming features). You may not use other references, as the playing field must be level for everyone. Collaboration is strictly forbidden. (I mean, it's a final exam, after all.) If you have any questions, please don't hesitate to email me: dsavitt@math.mcgill.ca.

The exam must be turned in to me by 4 p.m. on Friday, April 19th. I will be in my office at 4 p.m. to receive the exam. For each minute past 4:15 p.m. by my watch, 2 points will be deducted from your exam score.

The Questions:

1. Is 1066 congruent to a square modulo 4713? Prove your answer.
2. I am thinking of a real number which is the root of a quadratic polynomial with integer coefficients. This number has decimal expansion which begins 3.806659275674... Do you have any guesses as to exactly what number I'm thinking of?
3. Suppose p is a prime number such that:
 - 7 is a square (mod p),
 - $p \equiv 8 \pmod{15}$, and
 - the remainder when p is divided by 42 is a single-digit number.

What is $p \pmod{420}$?

4. The *Fibonacci sequence* is defined as follows: $F_{-1} = 1, F_0 = 0$, and $F_n = F_{n-1} + F_{n-2}$ for integers $n > 0$. For example, the sequence continues 1, 1, 2, 3, 5, ...
 - (a) (3 points) Suppose $b \geq a$ are non-negative integers. Using induction on a , establish the relation: $F_b F_{a-1} - F_a F_{b-1} = (-1)^a F_{b-a}$.
 - (b) (2 points) By the division algorithm, write $b = qa + r$ with $0 \leq r < a$. Using the relation in part (a), prove that if $n \mid F_b$ and $n \mid F_a$, then $n \mid F_r$ as well.
 - (c) (2 points) Prove that if $a \mid b$, then $F_a \mid F_b$.
 - (d) (3 points) Conclude that $F_{(a,b)} = (F_a, F_b)$.
5. (a) (5 points) Exhibit the group $(\mathbb{Z}/936\mathbb{Z})^\times$ as a product of cyclic groups; that is, find integers d_1, \dots, d_r so that $(\mathbb{Z}/936\mathbb{Z})^\times \cong C_{d_1} \times \dots \times C_{d_r}$, where C_{d_i} denotes the cyclic group of order d_i .

- (b) (5 points) How many elements of order exactly 4 are there (mod 936)? (Recall that an element g of a group G with identity e is said to have order exactly n provided that $g^n = e$, but $g^k \neq e$ for $0 < k < n$.)
6. (a) (5 points) Find the smallest integer solution (x, y) to the Pell equation $x^2 - 61y^2 = +1$ with $y \neq 0$.
- (b) (3 points) Show that $x^2 - 34y^2 = -1$ has no integer solutions.
- (c) (2 points) Find a rational solution to $x^2 - 34y^2 = -1$. (So, this is an example of a Diophantine equation with rational solutions but no integer solutions.)
7. (a) (5 points) List all of the reduced binary quadratic forms of discriminant $D = -160$.
- (b) (5 points) Prove that a prime number p other than 5 is represented by the form $5x^2 + 8y^2$ if and only if $p \equiv 13b^2 \pmod{160}$ or $p \equiv 13b^2 + 40 \pmod{160}$ for some b relatively prime to 160. (For example, $37 \equiv 13 \cdot 7^2 + 40 \pmod{160}$ and $37 = 5 \cdot 1^2 + 8 \cdot 2^2$.)
8. Let α be an irrational algebraic number; that is, α is irrational, but is the root of a polynomial with integer coefficients. You may use the following fact without proof: there is a polynomial $f(x)$ with integer coefficients such that:
- (i) α is a simple root of $f(x)$, i.e. $f(\alpha) = 0$ but $f'(\alpha) \neq 0$, where $f'(x)$ denotes the derivative of $f(x)$, and
- (ii) $f(x)$ has no rational roots.
- Now:
- (a) (5 points) Suppose the polynomial $f(x)$ has degree n . Prove that there exists a constant $c > 0$ such that $|\alpha - \frac{p}{q}| > \frac{c}{q^n}$ for all integers p, q . (Hint: can you put a lower bound on $|f(\frac{p}{q})|$?)
- (b) (2 points) Suppose α is an irrational number and suppose that for all integers n and positive real numbers c there exist p, q such that $|\alpha - \frac{p}{q}| < \frac{c}{q^n}$. Conclude that α cannot be an algebraic number. (Such α is called transcendental.)
- (c) (3 points) Show that $\alpha = \sum_{n=1}^{\infty} \frac{1}{10^{n!}}$ is a transcendental number.
9. Let n be a positive integer, and suppose that $x^2 + x + n$ is prime for all integers x in the range $0 \leq x < \sqrt{n/3}$. Prove that $x^2 + x + n$ is actually prime for all integers x in the range $0 \leq x < n - 1$. (Hint: try to list all reduced binary quadratic forms of discriminant $D = 1 - 4n$. Note that the middle coefficient b must be odd, so write $b = 2b' + 1$.)
10. (a) (5 points) Let n be a positive integer. Show that there exists an integer d such that the last n digits of 2^d are all either 1 or 2. (For example, if $n = 2$, one may take $d = 9$, as $2^9 = 512$.)
- (b) (5 points) For $n = 3$, what is the smallest such d ?