MA357, Spring 2020 — Midterm Exam

This is a take-home test. It is due no later than April 3.

The test contains 11 questions, but you do not have to solve all of them. The number of points for each question is indicated. You should solve enough problems to get at least 100 points, but the total value of the problems (full problems, not fractions of problems) you turn in can be no more than 120 points. The maximum score you can get is 100, so doing an extra 20 points' worth only buys you insurance. When I grade, I will go until I have graded problems worth up to the limit of 120 points, then stop.

Rules of the Game: While you work on this test, you may consult the textbook, your class notes and the material posted on the top half of the course web page (e.g., solutions to problem sets). You may use *Sage* or GP or other mathematical software to do computations. No other reference materials are allowed. In particular, you should not search the internet for solutions.

You should work entirely by yourself. You may talk to me (though I don't promise to answer every question you might have), but you may not talk to anyone else. (Complaining and asking for sympathy are ok, but don't discuss the actual content of the test.)

Finally, you should really *write up* (and not just write down) your solutions: they should read as if they were an example in a well-written textbook. Make sure that you explain carefully your line of reasoning at each point; your text should be such that another student at about your level could follow the steps without having to ask you for help. To achieve this goal, be as verbose as necessary — it is better to write too much than too little. Solutions should be written as carefully and legibly as possible. (The professor has old eyes.) *Don't turn in first-draft material.*

Together with your test, you should turn in a signed statement saying that you have followed the test rules as stated above.

Good luck!

> Number theorists are like lotus-eaters — having once tasted of this food they can never give it up.
>
> – Leopold Kronecker

1. **[15 points]** Show that the equation $x^2 + xy - y^2 = 3$ does not have integer solutions.

2. **[15 points]** A number n is called a *Carmichael number* if it is not prime but nevertheless we have $a^{n-1} \equiv 1 \pmod{n}$ for all numbers a which are relatively prime to n. Show that 6601 is a Carmichael number.

3. **[15 points]** For each positive integer k, let M_k be the number whose representation in base 10 is a string of k 9s in a row. So $M_1 = 9$, $M_2 = 99$, $M_8 = 99,999,999$. Let p be a fixed prime, $p > 5$. Show that there exist infinitely many k for which p divides M_k.

4. **[20 points]** (Fermat's trick for factoring Mersenne numbers.) Suppose p and q are odd primes, and q divides $2^p - 1$. Prove that there exists a k such that $q = 2kp + 1$. Explain how one might use this result to show (without using a computer) that $2^{17} - 1$ is prime.

(Hint for the proof: what is the order of 2 modulo q?)

5. **[25 points]** Does there exist an integer $m \geqslant 2$ such that $2^m \equiv 1 \pmod{m}$? (It is easy to guess the right answer to this one, but not so easy to prove the answer is right.)

6. **[15 points]** Show that $\phi(2^n - 1)$ is divisible by n. (Think about the order of 2 mod n.)

7. **[15 points]** Show that for any positive integer n, the number $1^n + 2^n + 3^n + 4^n$ is divisible by 5 if and only if n is not divisible by 4.

8. **[10 points]** Find the integers x such that

$$304x^{303} + 204x^{202} - 104x^{101} \equiv 0 \pmod{101}.$$

(Yes, one can do this by brute force, but try to be smarter than that.)

9. **[30 points]** Let p be an odd prime and let $g \in U_p$ be an element of order $p - 1$, so that $g^{p-1} \equiv 1 \pmod{p}$ (as it must) and $a^k \not\equiv 1 \pmod{p}$ if $0 < k < p - 1$. Such a g is called a *primitive root* mod p.

a. Show that every $a \in U_p$ is congruent to some power of g.

b. Define the *index* of a with respect to g to be the number i such that $a = g^i$ in $\mathbb{Z}/p\mathbb{Z}$:

$$\operatorname{ind}(a) = i \iff a \equiv g^i \pmod{p}.$$

Explain why we should consider $\operatorname{ind}(a)$ to be defined (mod $p - 1$).

c. Show that $\text{ind}(ab) \equiv \text{ind}(a) + \text{ind}(b) \pmod{p-1}$.

d. Show that $\text{ind}(-1) \equiv \frac{p-1}{2} \pmod{p-1}$.

e. Show that there exists an x such that $a \equiv x^2 \pmod{p}$ if and only if $\text{ind}(a)$ is even.

f. When is -1 a square (mod p)?

10. [30 points] I have taken a message, written it out in lower-case letters ignoring spaces and punctuation, and turned it into a string of numbers using the correspondence

$$a = 11 \qquad b = 12 \qquad c = 13 \qquad \ldots \qquad z = 36.$$

The resulting string was broken into blocks of digits, nine blocks in all. The ninth block may have been padded with 000s to make it as long as the rest.

To encrypt my message, I used the RSA method, with

$$m = 989779843544867054886292535108891926352726872 9$$

and encoding key

$$k = 230179247954559324470852582380776939286366561.$$

So I replaced each block a with the result of computing a^k modulo m. You can see the result below.

As we discussed in class, to decode the message you need to factor m. But m has only 46 digits, so any good mathematical software (such as *Sage*, GP, or *Mathematica*) will factor it.

So do it: factor m and decode the message.

423674261589028508788302770629935509259709611 1
174044901920174697383506798639879199201515788 4
936654741312859218196708454496670338435248854 0
825389798417504525250362157278040821963796090 5
185818271756437650274157164357009362248578000 2
951236540470452179200210670312291634950864183 8
313202252926391439391923253160009016059145487 5
592663805991044899889214213146661907112268039 9
447305912715674521503737967590540799107736906 4

For extra credit, identify the source of the quote.

11. [40 points] For this problem, we have to make or recall several definitions about real-valued functions defined on the positive integers $\mathbb{N}$.

First, a function $f : \mathbb{N} \longrightarrow \mathbb{R}$ is called *multiplicative* if we have $f(mn) = f(m)f(n)$ whenever $\gcd(m, n) = 1$. For example, we showed in class that φ is multiplicative and in one of the problem sets you checked that σ_0 is multiplicative. A simpler example of a multiplicative function is $f(n) = n$.

Second, the μ function is the multiplicative function defined by

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ (-1)^k & \text{if } n \text{ is the product of } k \text{ distinct primes} \\ 0 & \text{if } n \text{ is divisible by the square of some prime.} \end{cases}$$

Third, let's define two fairly simple multiplicative functions: $I(n)$ is equal to 1 if $n = 1$ and to 0 otherwise, and $u(n) = 1$ for all n.

Finally, if f and g are any two functions from $\mathbb{N}$ to $\mathbb{R}$, we define the *Dirichlet convolution* of f and g to be the function $f * g$ defined by

$$(f * g)(n) = \sum_{d|n} f(d)g(n/d),$$

i.e., to compute $f * g$ at an integer n we sum the values $f(d)g(e)$ as d and e run through pairs of positive integers such that $de = n$.

a. Show that μ is multiplicative.

b. Suppose $f : \mathbb{N} \longrightarrow \mathbb{R}$ is any function. What is $f * I$ equal to?

c. Show that $f * g = g * f$ for all functions $f, g : \mathbb{N} \longrightarrow \mathbb{R}$.

d. Show that $(f * g) * h = f * (g * h)$ for all functions $f, g, h : \mathbb{N} \longrightarrow \mathbb{R}$.

e. Show that if f and g are multiplicative, then $f * g$ is multiplicative.

f. What is $\mu * u$ equal to? (Use the previous result!)

g. The *Möbius inversion formula* says that if f is a multiplicative function and F is defined by

$$F(n) = \sum_{d|n} f(d),$$

then

$$f(n) = \sum_{d|n} \mu(d)F(n/d),$$

and conversely. Prove this. (Find a way to use the previous parts of this problem.)

h. In the Möbius Inversion Formula, do we really need to assume f is multiplicative?