MAT 475 WEEK 5: NUMBER THEORY

JACOB TSIMERMAN

These are way too many problems to consider. Just pick a few problems you like and play around with them. You are not allowed to try a problem that you already know how to solve. Otherwise, work on the problems you want to work on.

1. The Hints:

Work in groups. Try small cases. **Plug in small numbers.** Do examples. Look for patterns. Draw pictures. Use LOTS of paper. Talk it over. Choose effective notation. Look for symmetry. Divide into cases. Work backwards. Argue by contradiction. Consider extreme cases. Modify the problem. Generalize. Don't give up after five minutes. Don't be afraid of a little algebra. Sleep on it if need be. Ask.

2. Euclids algorithm

The *greatest common divisor* of two positive integers m, n, written $gcd(m, n)$, is the largest number k such that m and n are both divisible by k. It also happens to be the smallest positive integer which can be written as $am - bn$ for (not necessarily positive!) integers a, b. There is a famous algorithm known as Euclids algorithm to find k. It goes as follows: Start with the pair (m, n). Then if $m > n$, replace m by $m - n$. Otherwise, replace n by $n - m$. Continue until both numbers are equal, and the result is k. For instance, suppose $(m, n) = (105, 75)$. Then the algorithm goes as follows:

$$(105, 75) \to (30, 75) \to (30, 45) \to (30, 15) \to (15, 15)$$

so we learn that $gcd(105, 75) = 15$. In fact, we can speed this algorithm up by doing the following: instead of replacing m by $m - n$, we immediately replace m by the remainder of m when divided by n. This ends up being incredibly quick, and is how computers work out the *gcd*.

Some tricks to look for:

- Use the thereom of unique factorization: Every positive integers can be written as a product of prime powers in a unique way.
- Use modular arithmetic. That is, computer numbers modulo other numbers.
- Remember Fermat's Little Theorem: if m, p are positive integers with p a prime number, then $m^p = m \mod p$.

- Here's a neat trick: the sum of the digits of a positive integer has the same remainder modulo 9 as the original integer! This comes up a lot.
- Use size to your advantage. If A is much bigger than B, then there is no way these two could be equal! Practise example: find all positive integers N such that $N^3 + 5 = 4N^2 + 7$.

Here are some problems to get you started:

(1) Show that $n^7 - n$ is divisible by 42 for any positive integer n.
(2) If p and $p^2 + 2$ are primes, show that $p^3 + 2$ is prime.
(3) A triangular number is a positive integer of the form $\frac{n(n+1)}{2}$ for some positive integer n. So the triangular numbers are $1, 3, 6, 10, 15, \ldots$. Prove that m is a sum of two triangular numbers if and only if $4m+1$ is a sum of two squares.
(4) Define the following strange function on the positive integers. $F(n)$ is defined to be the number of digits of 5^n in base 10 plus the number of digits of 2^n in base 10. Notice that $F(1) = 2, F(2) = 3, F(3) = 4, F(5) = 5$. Prove that $F(n) = n + 1$ for every positive integer n.

2.1. **Problems to follow up on.** :

(1) Show that $n^{15} - n^3$ is divisible by 10 for any positive integer n.
(2) Find all prime numbers p such that $p^4 + 14$ is a prime.
(3) m, n are positive integers, each of which can be written as a sum of two squares. Prove that mn can also be written as a sum of two squares.
(4) Prove that there is no power of 10 whose decimal expansion in base 5 starts $444\ldots$ and whose decimal expansion in base 2 starts $111\ldots$.

2.2. **Number Theory Problems.** These are in increasing order of difficulty. The ones at the end are extremely challenging!

(1) How many zeroes are there at the end of $2015! = 1 \cdot 2 \cdot 3 \cdot 4 \cdots 2015$?
(2) Prove that for $n > 1$, the numbers $n! + 2, n! + 3, \ldots, n! + n$ are not prime.
(3) Derive a divisibility criterion for 11 in terms of the decimal expansion.
(4) Show that for any prime $p > 5$ there is a positive integer N whose decimal expansion consists of all 1's such that N is divisible by p.
(5) Prove that every positive integer n can be written as a quotient of a product of factorials of primes. For example,

$$1 = \frac{2!}{2!}, 2 = 2!, 3 = \frac{3!}{2!}, 4 = 2! \cdot 2!, 180 = \frac{5! \cdot 3!}{2! \cdot 2!}.$$

(6) Prove that if $m \mid (m-1)! + 1$ then m is prime.
(7) Prove that if $2^n - 1$ is prime, then n is prime.

(8) How many prime numbers, written in base 10, are such that their digits alternate 1's and 0's, beginning and ending with 1? For instance, 101 is prime, while $10101 = 91 \cdot 111$ is not. *Hint: use a geometric series*

(9) Let $r(n)$ be the sum of the remainders when n is divided by $1, 2, 3, \ldots, n$. Prove that for infinitely many positive integers k, we have $r(k) = r(k+1)$.

(10) Define the following function. If n is a positive integer, take m^2 to be the largest integer square with $m^2 \leq n$, and write $F(n) = n + (n - m^2)$. So $F(1) = 1, F(2) = 3, F(3) = 5, F(4) = 4, \ldots$. For which positive integers n, does the sequence $n, F(n), F(F(n)), F(F(F(n))), \ldots$ contain a square?

(11) Suppose that $n > 4$ is a positive integer. Prove that $n^4 + 4^n$ is not prime.

(12) Let m be the number $11111\ldots111$ with 2014 digits, all of them 1. What is the 1008'th digit of $\sqrt{m}$ after the decimal point?

(13) Suppose α, β are positive irrational numbers with $\frac{1}{\alpha} + \frac{1}{\beta} = 1$. Consider the two sequences $\lfloor n\alpha \rfloor$ and $\lfloor m\beta \rfloor$, in other words $\lfloor \alpha \rfloor, \lfloor 2\alpha \rfloor, \lfloor 3\alpha \rfloor \ldots$ and $\lfloor \beta \rfloor, \lfloor 2\beta \rfloor, \lfloor 3\beta \rfloor \ldots$. Prove that every positive integer occurs in exactly one of these sequences.

(14) Find all positive integers a, b, m, n with m relatively prime to n such that $(a^2 + b^2)^m = (ab)^n$.

(15) Let $a_1, a_2, \ldots, a_{n+1}$ be a sequence of positive integers with $a_1 = a_{n+1}$. Prove that

$$\prod_{i=1}^{n} (a_i + 2a_{i+1})$$

is not a power of 2.

(16) (HARD!) Let $p > 3$ be a prime. Prove that there exists a positive integer $n < p - 1$ such that neither of $n^{p-1} - 1$ and $(n+1)^{p-1} - 1$ are not divisible by p^2.