Math 250: Number Theory
Instructor: David Zureick-Brown ("DZB")

All assignments
Last updated: March 10, 2024
Gradescope code: ZWK583

Show all work for full credit!
Proofs should be written in full sentences whenever possible.

Contents

Assignment 1: Introduction to course; squares, triangles, and Pythagorean triples.

Due by 11:25am, eastern, on Thursday, Feb 08

Suggested readings for this problem set: Chapters 1, 2, 3. (Chapter 4 is bonus content.)
All readings are from Silverman, *A Friendly Introduction to Number Theory*.

Assignment: due Thursday, Feb 08, 11:25am, via Gradescope (ZWK583):

1. For each of the lists of numbers, (a) find the next three numbers and (b) find a formula for the nth term in the sequence. Describe the sequence in plain English too, if possible.

   (a) $7, 14, 21, 28, 35, \ldots$

   (b) $1, 4, 7, 10, 13, \ldots$

   (c) $1, 8, 27, 64, 125, \ldots$

   (d) $2, 4, 8, 16, 32, 64, \ldots$

   (e) $11, 20, 29, 38, 47, \ldots$

2. Try adding up the first few odd numbers and see if the numbers you get satisfy some sort of pattern. Once you find the pattern, express it as a formula. Give a geometric verification that your formula is correct.

3. The consecutive odd numbers 3, 5, and 7 are all primes. Are there infinitely many such "prime triplets"? That is, are there infinitely many prime numbers p such that $p + 2$ and $p + 4$ are also primes?

4. It is generally believed that infinitely many primes have the form $N^2 + 1$, although no one knows for sure.
   (a) Do you think that there are infinitely many primes of the form $N^2 - 1$?
   (b) Do you think that there are infinitely many primes of the form $N^2 - 2$?
   (c) How about of the form $N^2 - 3$? How about $N^2 - 4$?
   (d) Which values of a do you think give infinitely many primes of the form $N^2 - a$?

   Hint: work out several examples by hand, or with a computer (try using the code

   ```
   {n : n in [1..100] | IsPrime(n^2+1)};
   ```

   at the site http://magma.maths.usyd.edu.au/calc/)

5. A natural number is called **perfect** if it is equal to the sum of its "proper" divisors ("proper" means smaller). For example, $6 = 1 + 2 + 3$ so 6 is a perfect number. Find the next perfect number after 6 on your own, then look up the next few perfect numbers after that. Is there a general pattern to these numbers?

6. Recall that $(a, b, c) \in \mathbb{Z}^3$ is a **Pythagorean triple** if each of a, b and c are positive integers and $a^2 + b^2 = c^2$.

   (a) Do there exist any Pythagorean triples such that $c = 1$? Prove your answer.

   (b) Do there exist any Pythagorean triples such that $a = 1$? Prove your answer.

7. Suppose that (a, b, c) is a Pythagorean triple such that a is prime. Prove that $c = b + 1$.

8. (a) Use the lines through the point (1, 1) to describe all the points on the circle $x^2 + y^2 = 2$ whose coordinates are rational numbers.

   (b) What goes wrong if you try to apply the same procedure to find all the points on the circle $x^2 + y^2 = 3$ with rational coordinates?

Assignment 2: Divisibility and primality

Due by 11:25am, eastern, on Thursday, Feb 15

Suggested readings for this problem set: Chapters 5 and 6

All readings are from Silverman, *A Friendly Introduction to Number Theory*.

Assignment: due Thursday, Feb 15, 11:25am, via Gradescope (ZWK583):

---

1. Prove that if $a \mid b$ and $b \mid a$, then $a = b$ or $a = -b$.
2. Suppose that $a \mid b$. Prove that for all $n \in \mathbb{Z}_{>0}$, $a^n \mid b^n$.
3. Prove that if $ac \mid bc$ and $c \neq 0$, then $a \mid b$.
4. (a) Prove that for all $k \in \mathbb{N}$, 9 divides $10^k - 1$.

   (b) Use this to prove the "divisible by 9" detector: for any $n \in \mathbb{N}$, with digits a_0 (the 1s digit), a_1 (the 10s digit), a_2 (the 100s digit), etc. (i.e., $n = \sum 10^i a_i$), if $m = a_0 + a_1 + a_2 + \ldots + a_k$ (where a_k is the first digit of n) then n is divisible by 9 if and only if the m (the sum of its digits) is also divisible by 9.
5. There is a divisibility rule for 8 which uses the last **three** digits (compared to the rule for 4, which only used the last **two** digits). Figure out what the rule is, then prove that your rule is correct.

   (Optional: is there a rule for divisibility by 16? 32? 65536?)
6. Find all integers $n \geq 1$ so that $n^2 - 1$ is prime. Hint: factor $n^2 - 1$
7. Suppose that a and n are integers that are both at least 2. Prove that if $a^n - 1$ is prime, then $a = 2$ and n is a prime. (Primes of the form $2^n - 1$ are called Mersenne primes.)
8. Let n be an integer greater than ~~1~~ 2.[1] Prove that if one of the numbers $2^n - 1, 2^n + 1$ is prime, then the other is composite.

[1] There was a typo on the original version of this problem. In the correct problem, n should be greater than 2.

Assignment 3: Euclidean algorithm and linear equations

Due by 11:25am, eastern, on Thursday, Feb 22

Suggested readings for this problem set: Chapter 5 and 6

All readings are from Silverman, *A Friendly Introduction to Number Theory*.

Assignment: due Thursday, Feb 22, 11:25am, via Gradescope (ZWK583):

1. Use the Euclidean algorithm to compute each of the following gcd's.
   (a) gcd(12345,67890)
   (b) gcd(54321,9876)
2. How many divisors $d \in \mathbb{N}$ does $n = 1000$ have?
3. Find all positive integers a and b such that $\gcd(a, b) = 10$ and $\operatorname{lcm}(a, b) = 100$.
4. True or False. (If true, give a proof; if false, give a counterexample.) Let a, b be positive integers.
   (a) If $\gcd(a, b) = 1$, then $\gcd(a + b, ab) = 1$.
   (b) If $\gcd(a + b, ab) = 1$, then $\gcd(a, b) = 1$.
   (c) If $\gcd(a, b) = 5$, then $\gcd(a + b, ab) = 5$.
   (d) If $\gcd(a + b, ab) = 5$, then $\gcd(a, b) = 5$.

   Let $a, b, c \in \mathbb{Z}$. Some of the following problems are doable with just the definition of gcd, and some need Theorem 6.1 from our book (the Linear Equation Theorem).
5. Suppose a and b both divide c and $\gcd(a, b) = 1$. Prove that ab divides c.
6. Suppose that $\gcd(a, c) = 1$ and $\gcd(b, c) = 1$. Prove that $\gcd(ab, c) = 1$.
7. Let $a, b \in \mathbb{Z}$ with $\gcd(a, b) = d$. Prove that $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.
8. Let $k \in \mathbb{Z}$. Prove that $\gcd(2k + 1, 9k + 4) = 1$.

Assignment 4: Factorization and FTA

Due by 11:25am, eastern, on Thursday, Feb 29

Suggested readings for this problem set: Chapters 7 and 12

All readings are from Silverman, *A Friendly Introduction to Number Theory*.

Assignment: due Thursday, Feb 29, 11:25am, via Gradescope (ZWK583):

1. Start with the list consisting of the single prime {5} and use the ideas in Euclid's proof (Theorem 12.1 of our book) that there are infinitely many primes to create a list of primes until the numbers get too large for you to easily factor. (You should be able to factor any number less than 1000.)

2. Recall that the number *n factorial*, which is written $n!$, is equal to the product

$$n! = 1 \cdot 2 \cdot 3 \cdots (n-1) \cdot n.$$

   Find the highest power of 2 dividing each of the numbers $1!, 2!, 3!, \ldots, 10!$.

3. Formulate a rule that gives the highest power of 2 dividing $n!$. Use your rule to compute the highest power of 2 dividing 100! and 1000!.

4. Find a prime p such that the remainder when you divide p by 1115 is 223 (i.e., there is an integer k such that $p = 1115k + 223$). Are there infinitely many such primes?

5. Find a prime p such that the remainder when you divide p by 1115 is 323 (i.e., there is an integer k such that $p = 1115k + 323$). Are there infinitely many such primes?

6. Recall from last week's homework that $\gcd(12345, 67890) = 15$. Describe all integers $x, y \in \mathbb{Z}$ such that $12345x + 67890y = 15$.

7. Are there any integers n such that $7^n + 6^n$ and $7^n - 6^n$ are both prime? If so, give an example, and if not, give a proof that there are no such n.

8. Find all integers n such that $n + 1$ divides $n^2 + 1$. (Hint: use the division algorithm.)

Assignment 5: Modular Arithmetic

Due by 11:25am, eastern, on Thursday, Mar 07

Suggested readings for this problem set: Chapter 8

All readings are from Silverman, *A Friendly Introduction to Number Theory*.

Assignment: due Thursday, Mar 07, 11:25am, via Gradescope (ZWK583):

1. Let $p \neq q$ be two primes. Suppose that $p \mid a$ and $q \mid a$. Use Euclid's lemma to prove that that $pq \mid a$.
2. Let $p \neq q$ be two primes and suppose that $a \neq 0$. Suppose that $p \mid a$ and $q \mid a$. Use the fundamental theorem of arithmetic to prove that that $pq \mid a$.
3. Compute the following.
   (a) $15^{17} \mod 7$
   (b) $6^{28} \mod 15$
   (c) $7^{2018} \mod 100$
4. Suppose that $a_1 \equiv b_1 \pmod{m}$ and $a_2 \equiv b_2 \pmod{m}$. Prove that $a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$ and $a_1 - a_2 \equiv b_1 - b_2 \pmod{m}$.
5. Suppose that $a_1 \equiv b_1 \pmod{m}$ and $a_2 \equiv b_2 \pmod{m}$. Prove that $a_1 a_2 \equiv b_1 b_2 \pmod{m}$.
6. Suppose that $ac \equiv bc \pmod{m}$ and also assume that $\gcd(c, m) = 1$. Prove that $a \equiv b \pmod{m}$.
7. Prove that the number a is divisible by 11 if and only if the alternating sum of the digits of a is divisible by 11. (If the digits of a are $a_1 a_2 a_3 \ldots a_{d-1} a_d$, the alternating sum means to take $a_1 - a_2 + a_3 - \ldots$ with alternating plus and minus signs. Also: use the fact that $1001 = 7 \cdot 11 \cdot 11$)
8. Show that every integer of the form $4 \cdot 14^k + 1$, $k \geq 1$ is composite. Hint: use modular arithmetic to show that there is a factor of 3 when k is odd and a factor of 5 when k is even.

Midterm 1 study guide

In class on Thursday, Mar 14

Content: The questions will all be either

1. homework problems,
2. suggested problems,
3. problems we worked in class, or
4. minor variations of one of these.

Problems with very long proofs or that involved some unusual trick will not be on the exam.

You are allowed to use any previous problem from class or from the homework (e.g., "additivity of divisibility" or "the 2 out of 3 rule") on the exam without reproving it, unless otherwise noted on the exam. (E.g., if I ask you to prove "additivity of divisibility" on the exam, you will need to prove this using only the definition of divisibility, and I will remind you of this in the statement of the problem.)

A typical exam will have one or two questions from each week of the course and will cover **assignments 1-5**. You can expect problems about following:

- Divisibility
- GCD
- Euclidean Algorithm
- Linear Equations
- Prime numbers
- Modular arithmetic

Some problems will be calculations, e.g., compute $2^{100} \mod 11$, or $\gcd(12345, 67890)$. Some will be proofs of basic properties (like additivity of transitivity of divisibility, or Euclid's lemma). Most of the problems won't be very long (e.g., I will not ask you to paramaterize pythagorean triples), but I might include one medium length proof (like the infinitude of primes).

For definitions, I want a definition, in prose (complete sentences), and I want "just" the definition, and not any additional facts about the definition. (E.g., if you give the definition of rational, do not include that a rational number can be written in reduced form; that is a fact about rational numbers and not part of the definition of rational.)

Assignment 6: Modular linear equations

Due by 11:25am, eastern, on Thursday, Mar 28

Suggested readings for this problem set: Chapters 9 and 10.
All readings are from Silverman, *A Friendly Introduction to Number Theory*.

Assignment: due Thursday, Mar 28, 11:25am, via Gradescope (ZWK583):

IN PROGRESS! Check back later for the final assignment.

IN PROGRESS! Check back later for the final assignment.

Assignment 7: Fermat's little theorem

Due by 11:25am, eastern, on Thursday, Apr 04

Suggested readings for this problem set: TBA

All readings are from Silverman, *A Friendly Introduction to Number Theory*.

Assignment: due Thursday, Apr 04, 11:25am, via Gradescope (ZWK583):

Assignment 8: TBA

Due by 11:25am, eastern, on Thursday, Apr 11

Suggested readings for this problem set: TBA
All readings are from Silverman, *A Friendly Introduction to Number Theory*.

Assignment: due Thursday, Apr 11, 11:25am, via Gradescope (ZWK583):

IN PROGRESS! Check back later for the final assignment.

Assignment 9: TBA

Due by 11:25am, eastern, on Thursday, Apr 18

Suggested readings for this problem set: TBA
All readings are from Silverman, *A Friendly Introduction to Number Theory*.

Assignment: due Thursday, Apr 18, 11:25am, via Gradescope (ZWK583):

Assignment 10: TBA

Due by 11:25am, eastern, on Thursday, Apr 25

Suggested readings for this problem set: TBA

All readings are from Silverman, *A Friendly Introduction to Number Theory*.

Assignment: due Thursday, Apr 25, 11:25am, via Gradescope (ZWK583):

IN PROGRESS! Check back later for the final assignment.

Midterm 2 study guide

In class on Thursday,

Content: The questions will all be either

1. homework problems,
2. suggested problems,
3. problems we worked in class, or
4. minor variations of one of these.

Problems with very long proofs or that involved some unusual trick will not be on the exam.

You are allowed to use any previous problem from class or from the homework (e.g., "additivity of divisibility" or "the 2 out of 3 rule") on the exam without reproving it, unless otherwise noted on the exam. (E.g., if I ask you to prove "additivity of divisibility" on the exam, you will need to prove this using only the definition of divisibility, and I will remind you of this in the statement of the problem.)

A typical exam will have one or two questions from each week of the course. You can expect problems about following:

- TBA

For definitions, I want a definition, in prose (complete sentences), and I want "just" the definition, and not any additional facts about the definition. (E.g., if you give the definition of rational, do not include that a rational number can be written in reduced form; that is a fact about rational numbers not part of the definition of rational.)

Assignment 11: TBA

Due by 11:25am, eastern, on Thursday, May 02

Suggested readings for this problem set: TBA

All readings are from Silverman, *A Friendly Introduction to Number Theory*.

Assignment: due Thursday, May 02, 11:25am, via Gradescope (ZWK583):

IN PROGRESS! Check back later for the final assignment.

Assignment 12: TBA

Due by 11:25am, eastern, on Thursday, May 07

Suggested readings for this problem set: TBA

All readings are from Silverman, *A Friendly Introduction to Number Theory*.

Assignment: due Thursday, May 07, 11:25am, via Gradescope (ZWK583):

IN PROGRESS! Check back later for the final assignment.

Final exam study guide

Final exam is **May ???**, ???pm, in SMUD 014.

The **last day of class** is Tuesday, May 7.

There will be **office hours** on before the exam. I will send out a survey to find a time that works for everyone who is planning to attend.

The final exam will be comprehensive.
The exam will be, roughly 8-10 questions, with multiple parts. Some questions will be "prove or disprove". For disproofs, please write out a counterexample as your disproof.

A typical exam will have roughly one or two questions from each week of the course. You can expect a subset of the following:

- TBA

IN PROGRESS! Check back later for the final assignment.