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

All assignments
Last updated: May 5, 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 $\text{lcm}(a, b) = 100$.
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:

- Definitions (e.g., the definition of a divides b)
- Divisibility
- GCD and LCM
- 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: Chapter 8.
All readings are from Silverman, *A Friendly Introduction to Number Theory*.

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

1. (a) Suppose that $ac \equiv bc \mod m$ and also assume that $\gcd(c, m) = 1$. Prove that $a \equiv b \mod m$.
   (b) Suppose that $ac \equiv bc \mod m$ but also that $\gcd(c, m) > 1$. Is it still always true that $a \equiv b \mod m$? Prove or disprove your claim.

2. Find all incongruent solutions to each of the following linear congruences.
   (a) $21x \equiv 1 \mod 41$
   (b) $7x \equiv 3 \mod 15$
   (c) $823x \equiv 1 \mod 4526$
   (Hint[2]: .)

3. Find all incongruent solutions to each of the following linear congruences.
   (a) $6x \equiv 5 \mod 15$
   (b) $21x \equiv 14 \mod 91$
   (c) $66x \equiv 100 \mod 121$

4. Find all incongruent solutions to each of the following quadratic congruences.
   (a) $x^2 \equiv 2 \mod 7$
   (b) $x^2 \equiv 3 \mod 7$
   (c) $x^2 \equiv 1 \mod 8$

5. Determine the number of incongruent solutions for each of the following congruences.
   (a) $72x \equiv 47 \mod 200$
   (b) $4183x \equiv 5781 \mod 15087$
   (c) $1537x \equiv 2863 \mod 6731$

6. (a) Let N be a positive integer. What is the last digit of 2^N? (The last digit will depend on N; express your answer as a congruence condition on N.)
   (b) What is the last digit of $2^{2^{2^{2^{2^2}}}}$? (This is six 2's.)

7. What is $2^{2^{2^{2^{2^{2^2}}}}} \mod 11$? (This is seven 2's)

8. What is $2^{2^{2^{2^{2^{2^{2^2}}}}}} \mod 7$? (This is eight 2's.)

[2]The hint is in white; copy it and paste it in a text editor to see the hint.

Assignment 7: Fermat's little theorem

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

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

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

1. Prove that for all $n \in \mathbb{Z}_{\geq 0}$, $35 \mid 3^{6n} - 2^{6n}$. (Hint[3]: .)

2. (a) Compute $2^{-1} \bmod 7$.
   (b) Compute $2^{-1} \bmod 31$.
   (c) Compute $2^{-1} \bmod 11$.

3. (a) How many roots does the polynomial $x^2 + x + 1$ have mod 2?
   (b) How many roots does the polynomial $x^2 + x + 1$ have mod 3?
   (c) How many roots does the polynomial $x^2 + x + 1$ have mod 5?

4. (a) Compute $7^{222} \bmod 13$. (Final answer should be between 0 and 12.)
   (b) Compute $14^{15^{16}} \bmod 17$. (Final answer should be between 0 and 16.)

5. Your final answer for both parts of this problem should be between 0 and 16.
   (a) Solve the equation $x \cdot 15^{15} = 1 \bmod 17$ for x.
   (b) Compute $15^{15^{15}} \bmod 17$.

6. Let $p > 1$ be a prime. Prove that p does not divide $2^p - 1$. (Hint: .)

7. Recall from class that if $f(x) \in (\mathbb{Z}/p\mathbb{Z})[x]$, and if $r \in \mathbb{Z}/p\mathbb{Z}$ is a root (i.e., $f(r) = 0 \bmod p$), then $x - r$ divides $f(x) \bmod p$ (i.e., there exists a polynomial $g(x) \in (\mathbb{Z}/p\mathbb{Z})[x]$ such that $f(x) = (x - r)g(x)$.

   Show that the polynomial $x^{p-1} - 1$ factors (mod p) as

   $$x^{p-1} - 1 = (x - 1)(x - 2) \cdots (x - (p - 1)).$$

   Verify that this is true for $p = 5$ by multiplying out both sides. (Hint: .)

8. In class we proved Wilson's theorem: $(p - 1)!$ is congruent to $-1 \bmod p$. Suppose that n is **not** a prime.
   (a) Give a counterexample to show that $(n - 1)!$ is not congruent to $-1 \bmod n$.
   (There was a typo in the original version of this problem: the n in red was originally a p).
   (b) What are the possibilities for $(n-1)! \bmod n$? Do several examples; then make a guess, and prove that your guess is correct.

[3]The hint is in white; copy it and paste it in a text editor to see the hint

Assignment 8: Order, Fermat's little theorem, Euler's theorem

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

Suggested readings for this problem set: Chapters 9, 10, 11.
All readings are from Silverman, *A Friendly Introduction to Number Theory*.

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

1. Recall that **Euler's phi function** is the function $\phi(n) = (\mathbb{Z}/n\mathbb{Z})^*$ (i.e., the number of integers a between 0 and $n-1$ such that $\gcd(a,n) = 1$). Find the following values of $\phi(n)$:

   $$\phi(5), \phi(6), \phi(16), \phi(77), \phi(36).$$

   Recall that the **order** of an element $a \in (\mathbb{Z}/n\mathbb{Z})^*$ is the smallest positive integer i such that $a^i \equiv 1 \mod n$.

2. Find the order of of the following:

   (a) 4 mod 7;

   (b) 11 mod 60;

   (c) 37^{230} mod 100.

3. Find the order of every non-zero element of $(\mathbb{Z}/36\mathbb{Z})^*$.

4. Solve for x in the congruence $x^{17} \equiv 3 \mod 19$.

5. Let $a, n, k \in \mathbb{Z}$ be integers and suppose that the order of a mod n is prime p. What is the order of a^k? (This might depend on k.) Prove your claim.

6. Let $a, n \in \mathbb{Z}$ be integers and suppose that the order of a mod n is prime p. What is the order of a^p? Prove your claim.

7. A composite number m is called a **Carmichael number** if the congruence $a^{m-1} \equiv 1 \pmod{m}$ is true for every number a with $\gcd(a,m) = 1$.

   Verify that $m = 561 = 3 \cdot 11 \cdot 17$ is a Carmichael number. [Hint: It is not necessary to actually compute $a^{m-1} \pmod{m}$ for all 320 values of a. Instead, use Fermat's Little Theorem to check that $a^{m-1} \equiv 1 \pmod{p}$ for each prime p dividing m and then explain why this implies that $a^{m-1} \equiv 1 \pmod{m}$.]

8. Let $n > 1$ be an integer. Prove that n does not divide $2^n - 1$. (Hint:

   .)

Assignment 9: More order; fast squaring; a primality test; Multiplicativity of $\phi(n)$

*Due by **Friday**, 11:25am eastern, on Friday, April 19*

Suggested readings for this problem set: Chapters 16, 17 and 18
All readings are from Silverman, *A Friendly Introduction to Number Theory*.

Assignment: Due by **Friday**, 11:25am eastern, on Friday, April 19, via Gradescope (ZWK583):

1. Find a prime divisor p of $2^{23} - 1$. (This is 8388608; instead of factoring it, think about $o_p(2)$ like we did in class.)
2. Let a be an integer and let n, m be positive integers. What is $\gcd(a^n - 1, a^m - 1)$?. Prove that your answer is correct. (Hint: .)
3. Recall that if p is a prime number and if $a \not\equiv 0 \pmod{p}$ then Fermat's Little Theorem tells us that $a^{p-1} \equiv \pmod{p}$.
   (a) The congruence $7^{1734250} \equiv 1660565 \pmod{1734251}$ is true. Can you conclude that 1734251 is a composite number?
   (b) The congruence $129^{64026} \equiv 15179 \pmod{64027}$ is true. Can you conclude that 64027 is a composite number?
   (c) The congruence $2^{52632} \equiv 1 \pmod{52633}$ is true. Can you conclude that 52633 is a prime number?
4. Use the method of successive squaring (see Chapter 16) to compute each of the following:
   (a) $5^{13} \bmod 23$.
   (b) $28^{749} \bmod 1147$. (Feel free to use a calculator to help with this problem.)

Midterm 2 study guide

In class on Tuesday, Apr 23

Content: The questions will all be either

1. Definitions,
2. homework problems,
3. suggested problems,
4. problems we worked in class, or
5. 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.)

The exam will cover material from assignments 6-9 and from lectures those weeks. (But remember, some of those problems needed earlier material to solve, e.g. the Euclidean Algorithm.)

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

- Modular linear equations
- Solving congruence equations
- Inverses
- Fermat's little theorem
- Euler's theorem
- Order
- $\phi(n)$
- Computations involving powers
- Fast squaring
- Polynomials mod p
- Wilson's theorem.

One problem will be to prove one of the following theorems from class (your choice):

- Fermat's little theorem
- Euler's theorem
- Wilson's theorem.
- Chinese remainder theorem.

Assignment 10: Quadratic reciprocity

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

Suggested readings for this problem set: Chapters 20, 21, 22.
All readings are from Silverman, *A Friendly Introduction to Number Theory*.

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

1. Compute the following: $\left(\frac{85}{101}\right)$, $\left(\frac{29}{541}\right)$, $\left(\frac{101}{1987}\right)$, $\left(\frac{31706}{43789}\right)$. (The denominators are all prime.)
2. Do the following quadratic equations have a solution? (541 and 31957 are prime.) Edit: initially this problem said "solve"; don't solve them, just say whether there is a solution or not.
   (a) $x^2 \equiv -29 \mod 541$,
   (b) $x^2 - 3x - 1 \equiv 0 \mod 31957$.
3. Compute a formula for $\left(\frac{-3}{p}\right)$. (Your answer will have cases and depend on p mod 12.) Edit: Actually it only depends on p mod 3.
4. Suppose that p and q are twin primes (i.e., they are both prime, and $q = p + 2$). Is it possible that 2 is a quadratic residue for both p and q? Is 2 necessarily a quadratic residue of p or q? Find twin primes p and q such that 2 is a quadratic residue modulo p but not modulo q.

Assignment 11: Primitive roots

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

Suggested readings for this problem set: Chapters 28 sand 29.
All readings are from Silverman, *A Friendly Introduction to Number Theory*.

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

1. First, without solving them, how many incongruent solutions does each of the following congruences have? Second, find a primitive root mod 29, and use it to solve the following congruences:
   (a) $x^{28} \equiv 1 \mod 29$;
   (b) $x^3 \equiv 1 \mod 29$;
   (c) $x^7 \equiv 1 \mod 29$;
   (d) $x^6 \equiv 1 \mod 29$.
2. Let $n = 4p$, where p is a prime number. Show that there does not exist a primitive root mod n.
3. Let p and q be primes, and suppose that $p = 4q + 1$. Prove that 2 is a primitive root mod p.
4. (a) Let g be a primitive root mod a prime p. Solve the equation $g^x \equiv -1 \mod p$ for x.
   (b) For which primes p is it true that g is a primitive root mod p iff $-g$ is a primitive root mod p?

Final exam study guide

Final exam is **May 13**, 9-11am, in SMUD 014.

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

There will be **office hours** 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.

Content: The questions will all be either

1. Definitions,
2. homework problems,
3. suggested problems,
4. problems we worked in class, or
5. 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.)

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).

A typical exam will have one or two questions from each week of the course (with more emphasis on material since the most recent exam). You can expect problems about (a subset of) the following:

- Definitions (e.g., the definition of a divides b)
- Divisibility
- GCD and LCM
- Euclidean Algorithm
- Linear Equations
- Prime numbers
- Modular arithmetic

- Modular linear equations
- Solving congruence equations
- Inverses
- Fermat's little theorem
- Euler's theorem
- Order
- $\phi(n)$
- Computations involving powers
- Fast squaring
- Polynomials mod p
- Wilson's theorem.
- Quadratic reciprocity
- Primitive roots

TWO problems will be to state and prove two of the following theorems from class (your choice):

- Infinitude of the primes.
- Linear equation theorem (about when the linear equation $ax = b \mod n$ has a solution, and how many solutionts it has).
- Linear combination theorem ($ax + by = n$ has a solution if and only if $n \mid \gcd(a, b)$).
- Fundamental Theorem of Arithmetic.
- Fermat's little theorem
- Euler's theorem
- Wilson's theorem.
- Chinese remainder theorem.
- Let $\gcd(a, n) = 1$. Prove that $a^k \equiv 1 \mod n$ if and only if $o_n(a) \mid k$.
- Prove that primitive roots don't exist mod n if $n = 4p$.
- Euler's formula for $\left(\frac{a}{p}\right)$.
- State formula for $\left(\frac{-1}{p}\right)$ (the one with two cases) and prove that it is correct.