Number theory comments

Sophie Marques

Tuesday 21st October, 2014

Of course this does not cover all the class notes and it is not enough to do the midterm. It is just a way to extract the very important part of the course and I do not mean that you do not have to know the remaining part. THIS ARE NOT ALLOWED FOR THE MIDTERM, IF USED, 0 ON THE MIDTERM WILL BE APPLIED.

What are the essential definitions, properties results that you need to know?

Divisibility

Definition 0.0.1. *Let a and b be integers, $a \neq 0$.*
a divides b *or $a|b$ or* ***b is divisible by a*** *or* ***b is a multiple of a*** *or* ***a is a divisor of b*** *if there exist an integer c such that $b = ca$.*

Theorem 0.0.2. *Let a, b, c, x, y be integers.*

1. *If $a|b$, the $a|xb$.*
2. *If $a|b$ and $a|c$, then $a|bx + cy$.*
3. *If $a|b$ then $xa|xb$.*
4. *If $a|b$, then $|a| \leqslant |b|$. In particular, if $a|b$ and $b|a$, then $a = \pm b$.*

GCD and LCM

Definition 0.0.3. *Let a and b be integers, not both zeros. The* ***greatest common divisor*** *(also called* ***highest common factor****, abbreviated as G. C. D. or H. C. F.) of a and b, denoted as $gcd(a, b)$, is defined to be the largest integer which divides both a and b.*
That is $d = gcd(a, b)$.

1. *$d|a$ and $d|b$;*
2. *$d > 0$;*
3. *For any $d' \in \mathbb{Z}$ such that $d'|a$ and $d'|b$ then $d'|d$.*

Definition 0.0.4. *Let a and b be integers, not both zeros. The* ***lowest common divisor*** *(abbreviated as L. C. M.) of a and b, denoted as $lcm(a, b)$, is defined to be the largest integer which divides both a and b.*
That is $d = lcm(a, b)$.

1. *$a|d$ and $b|d$;*
2. *$d > 0$;*
3. *For any $d' \in \mathbb{Z}$ such that $a|d'$ and $b|d'$ then $d|d'$.*

Prime number

Definition 0.0.5. *We say that an integer $p > 1$ is a **prime integers** if its only divisors are 1 and itself.*
*An integer $n > 1$ which is not prim is said to be **composite**; such an integer integer has the form $n = ab$ where $1 < a < n$ and $1 < b < n$.*

Corollary 0.0.6. *Let a, b, c and m be non-zero integers. Then*

1. $gcd(ma, mb) = |m|gcd(a, b)$.
2. $gcd(a, m) = gcd(b, m) = 1$ *if and only if* $gcd(ab, m) = 1$,
3. $c|ab$ *and* $gcd(b, c) = 1$ *imply* $c|a$,
4. $a|c$, $b|c$ *and* $gcd(a, b) = 1$ *imply* $ab|c$
5. $gcd(a, b) = gcd(b, a) = gcd(a, b + ma)$,
6. $gcd(a, b)lcm(a, b) = |ab|$.

Lemma 0.0.7. *An integer $n > 1$ is composite if and only if it is divisible by some $p \leqslant \sqrt{n}$.*

Euclidean division

Lemma 0.0.8 (Existence and unicity of the Euclidean division)**.** *Let a and b be integers, $a \neq 0$. There exists unique integers q and r such that*

$$a = bq + r$$

with $0 \leqslant r < |a|$.

Euclidean algorithm

Theorem 0.0.9. *Let a and b be positive integers, $a > b$. Then we apply a series of divisions as follows.*

$$\begin{aligned}
a &= bq_0 + r_1 && 0 \leqslant r_1 < b,\\
b &= r_1q_1 + r_2 && 0 \leqslant r_2 < r_1,\\
r_1 &= r_2q_2 + r_3 && 0 \leqslant r_3 < r_2,\\
&\vdots\\
r_{n-2} &= r_{n-1}q_{n-1} + r_n && 0 < r_n < r_{n-1},\\
r_{n-1} &= r_nq_n.
\end{aligned}$$

The process of division comes to an end when $r_{n+1} = 0$. *The integer* r_n *is the G. C. D. of* a *and* b.

Bezout's identity

Theorem 0.0.10. *Let a and b be integers with $gcd(a,b) = d$. There exist integers u and v such that*

$$au + bv = d.$$

Such u, v can be obtained by backward tracing of the Euclidean divisions in finding the G. C. D, called **Extended GCD algorithm**.

Theorem 0.0.11. *Let a and b be integers (not both 0) with greatest common divisor d. Then, an integer c has the form $ax + by$ for some x, $y \in \mathbb{Z}$ if and only if c is a multiple of d. In particular, d is the least positive integer of the form $ax + by$ (x, $y \in \mathbb{Z}$).*

Corollary 0.0.12. *Two integers a and b are coprime if and only if there exist integers x and y such the*

$$ax + by = 1.$$

Linear diophantine equations

Theorem 0.0.13. *Let a, b and c be integers, with a and b not both 0, and let $d = gcd(a,b)$. Then the equation*

$$ax + by = c$$

has an integer solution x, y if and only if c is a multiple of d, in which case there are infinitely many solutions. There are the pairs

$$x = x_0 + \frac{bn}{d},\ y = y_0 - \frac{an}{d}\ (n \in \mathbb{Z}),$$

where x_0, y_0 is any particular solution.

The fundamental theorem of arithmetic

Lemma 0.0.14. *Let p be a prime, and let a and b any integers. Then either p divides a, or a and p are coprime;*

Lemma 0.0.15 (Gauss lemma)**.** *Let p be a prime, and let a and b any integers. Then p divides ab if and only if p divides a or p divides b.*

Theorem 0.0.16 (Fundamental theorem of arithmetic)**.** *Each integer $n > 1$ has a prime-power factorization*

$$n = p_1^{e_1} ... p_k^{e_k}$$

where $p_1, \ldots, p_k$ are distinct primes and $e_1, \ldots, e_k$ are positive integers; this factorization is unique, apart from permutations of the factors.

Remark 0.0.17. *The prime-power factorizations allows us to calculate products, quotients, powers, greatest common divisors and least common multiples. Suppose that integers a and b have factorizations*

$$a = p_1^{e_1} ... p_k^{e_k} \quad and \quad b = p_1^{f_1} ... p_k^{f_k}$$

(where we have e_i, $f_i \geqslant 0$ to allow for the possibility that some prime p_i may divide one but not both of a and b). Then we have

$$\begin{aligned} ab &= p_1^{e_1+f_1} ... p_k^{e_k+f_k}, \\ a/b &= p_1^{e_1-f_1} ... p_k^{e_k-f_k} \ (if \ b|a), \\ a^m &= p_1^{me_1} ... p_k^{me_k}, \\ gcd(a,b) &= p_1^{min(e_1,f_1)} ... p_k^{min(e_k,f_k)} \\ lcm(a,b) &= p_1^{max(e_1,f_1)} ... p_k^{max(e_k,f_k)} \end{aligned}$$

where $min(e,f)$ and $max(e,f)$ are the minimum and maximum of e and f.

Arithmetic functions

Definition 0.0.18. *An **arithmetic function** is a function $f : \mathbb{N} \to \mathbb{C}$.*

Definition 0.0.19. *Let f be an arithmetic function with $f(1) = 1$. Then f is called **multiplicative** if $f(mn) = f(m)f(n)$ for all m, n with $gcd(m,n) = 1$ and **strongly multiplicative** if $f(mn) = f(m)f(n)$, for all m, n.*

Convolution

Definition 0.0.20. *Let f and g be two arithmetic functions. Their **convolution product** denoted by $f \star g$ is defined by*

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

Theorem 0.0.21. *The convolution product of two multiplicative functions is again multiplicative.*

Möbius inversion

Definition 0.0.22. *The **Möbius function** $\mu(n)$ is defined by $\mu(1) = 1$, $\mu(n) = 0$ if n is divisible by a square > 1 and $\mu(p_1...p_t) = (-1)^t$ for any product of distinct primes $p_1, \ldots, p_t$.*

Theorem 0.0.23. *(Möbius inversion) Let f be an arithmetic function and let F be defined by*

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

Then, for any $n \in \mathbb{N}$,

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

Euler function

Definition 0.0.24. *We define* $\phi(n) = \{a \in \{1, ..., n\} | gcd(a, n) = 1\}$. *This function* ϕ *is called the* ***Euler's function****. For small* n*, its values are as follows.*

Theorem 0.0.25. *Let* ϕ *b the Euler* ϕ*-function. Then,*

1. $$n = \sum_{d|n} \phi(d), \ \forall n \geqslant 1$$

2. ϕ *is multiplicative.*

3. $$\phi(n) = n \prod_{p|n} (1 - 1/p)$$

Congruences

Definition 0.0.26. *Let n be a positive integer, and let a and b be any integers. We say that a **is congruent to** b **mod** (n), or a is a residue of b mod (n), written*

$$a \equiv b \ mod \ (n)$$

if one of the following equivalent assertions are satisfied:

1. *a and b leave the same remainder when divided n.*
2. *$r = r'$ where by the division algorithm, $a = qn + r$ with $a \leqslant r < n$, and $b = q'n + r'$ with $0 \leqslant r' < n$.*
3. *$n|(a - b)$*

DO NOT FORGET that $n|m$ if and only if $m \equiv 0 \ mod \ n$.

Lemma 0.0.27. *The congruence relation is a equivalence relation, that is: For any fixed $n \geqslant 1$ we have for any a, b and c integers:*

1. *$a \equiv a \ mod \ (n)$ (reflexivity);*
2. *if $a \equiv b \ mod \ (n)$ then $b \equiv a \ mod \ (n)$ (symmetry);*
3. *if $a \equiv b \ mod \ (n)$ and $b \equiv c \ mod \ (n)$ then $a \equiv c \ mod \ (n)$ (transitivity).*

Definition 0.0.28. *Let n be an integer. The equivalence class for the relation $\equiv$ mod (n) are called **congruence classes of** a **mod** (n). For some a integer,*

$$\text{we denote by } [a] \text{ (or sometimes } [a]_n)$$

its congruence classes of a mod (n), that is

$$\begin{aligned} [a] &= \{b \in \mathbb{Z} | a \equiv b \ mod \ (n)\} \\ &= \{...., a - 2n, a - n, a, a + n, a + 2n, ...\} \end{aligned}$$

*Each integer b such that $[b] = [a]$ is called a **representative of the class** $[a]$.*
We denote by $\mathbb{Z}/n\mathbb{Z}$ the set of all the classes of congruences mod (n).

Lemma 0.0.29. *Let a and b be integers, if $b \in [a]$ then $[a] = [b]$.*

Definition 0.0.30. *Let n be an integer. A set of n integers, containing one representative from each to the n congruence classes in $\mathbb{Z}/n\mathbb{Z}$ is called a* ***complete set of residues*** *mod (n).*

The integers $0, ..., n-1$ are called ***the least non-negative residues*** *mod (n).*

The integers r such that $-n/2 < r \leqslant n/2$ are ***the least absolute residue*** *mod (n).*

Lemma 0.0.31. *For n an integer,*

$$\mathbb{Z}/n\mathbb{Z} = \{[0], [1], ..., [n-1]\}$$

Lemma 0.0.32. *For a given $n \geqslant 1$, if $a' \equiv a \ mod\ (n)$ and $b' \equiv b \ mod\ (n)$ then,*

$$\begin{aligned} a' + b' &\equiv a + b \ \ mod\ (n) \\ a' - b' &\equiv a - b \ \ mod\ (n) \\ a' \cdot b' &\equiv a \cdot b \ \ mod\ (n) \end{aligned}$$

In other words, if a, a', b and b' are integers such that $[a] = [a']$ and $[b] = [b']$ then

$$\begin{aligned} [a+b] &= [a'+b'], \\ [a-b] &= [a'-b'], \\ [ab] &= [a'b']. \end{aligned}$$

Definition 0.0.33. *Let n be an integer.*

1. *We define an* ***addition*** *$+$ over $\mathbb{Z}/n\mathbb{Z}$, for any a and b, we put*

$$[a] + [b] := [a+b]$$

Similarly

$$[a] - [b] := [a-b]$$

2. *We define a* ***multiplication*** *$\cdot$ over $\mathbb{Z}/n\mathbb{Z}$, for any a and b, we put*

$$[a] \cdot [b] := [a \cdot b]$$

Lemma 0.0.34. *For any integers $a_1, \ \ldots\ , a_n$ and a,*

1. $[a_1] + [a_2] + ... + [a_n] = [a_1 + ... + a_n]$; $[a_1] \cdot [a_2] \cdot ... \cdot [a_n] = [a_1 \cdot ... \cdot a_n]$;
2. $[a]^k = [a^k]$.

Congruence equations

Theorem 0.0.35. *If $d = gcd(a, n)$, then the linear congruence*

$$ax \equiv b \ mod \ (n)$$

has a solution if and only if $d|b$. If d does divides b, and if x_0 is a particular solution, then the general solution is given by

$$x = x_0 + \frac{nt}{d}$$

where $t \in \mathbb{Z}$; in particular, the solutions form exactly d congruence classes mod (n), with representatives

$$x = x_0, x_0 + \frac{n}{d}, x_0 + \frac{2n}{d}, ..., x_0 + \frac{(d-1)n}{d}$$

Corollary 0.0.36. *If $gcd(a, n) = 1$ then the solution x of the linear congruence $ax \equiv b \ mod \ (n)$ form a single congruence class mod (n).*

Lemma 0.0.37. *1. Let m divide a, b and n, and let $a' = a/m$, $b' = b/m$ and $n' = n/m$, then*

$$ax \equiv b \ mod \ (n) \text{ if and only if } a'x \equiv b' \ mod \ (n')$$

2. Let a and n be coprime, let m divide a and b, let $a' = a/m$ and $b' = b/m$; then

$$ax \equiv b \ mod \ (n) \text{ if and only if } a'x \equiv b' \ mod \ (n)$$

Simultaneous linear congruence equations, chinese remainder theorem

Theorem 0.0.38. *Let n_1, n_2, ..., n_k be positive integers, with $gcd(n_i, n_j)$ whenever $i \neq j$, and let a_1, ..., a_k be any integers. Then the solutions of the simultaneous congruences*

$$x \equiv a_1 \ mod \ (n_1), \ x \equiv a_2 \ mod \ (n_2), ..., x \equiv a_k \ mod \ (n_k)$$

form a single congruence class $[x_0]$ mod (n), where $n = n_1 n_2 ... n_k$ (and

$$x_0 = a_1 c_1 d_1 + a_2 c_2 d_2 + ... + a_k c_k d_k$$

where $c_i = n/n_i$ and d_i is a solution of the congruence $c_i x \equiv 1 \ mod \ (n_i)$. In other words, the general solution is of the form $x = x_0 + nt$ where $t \in \mathbb{Z}$.

Corollary 0.0.39. *Let n have prime-power factorization*

$$n = p_1^{e_1} ... p_k^{e_k}$$

where p_1, ..., p_k are distinct primes. Then for any integers a and b we have $a \equiv b \ mod \ (n)$ if and only if $a \equiv b \ mod \ (p_i^{e_i})$ for each $i = 1, ..., k$.

On polynomial roots mod a prime

Theorem 0.0.40. *Let p be prime, and let $f(x) = a_d x^d + ... + a_1 x + a_0$ be a polynomial with integer coefficients, where $a_i \not\equiv 0 \ mod \ p$ for some i. Then, the congruence $f(x) \equiv 0 \ mod \ p$ is satisfied by at most d congruence classes $[x] \in \mathbb{Z}/p\mathbb{Z}$.*

Corollary 0.0.41. *Let $f(x) = a_d x^d + ... + a_1 x + a_0$ be a polynomial with integer coefficients, and let p be prime. If $f(x)$ has more than d roots in $\mathbb{Z}/p\mathbb{Z}$, then p divides each of its coefficients a_i*

Fermat's little theorem

Theorem 0.0.42 (Fermat's little theorem)**.** *If p is prime and $a \not\equiv 0 \ mod \ p$, then $a^{p-1} \equiv 1 mod \ p$.*

Corollary 0.0.43. *If p is prime then $a^p \equiv a \ mod \ (p)$ for every integer a.*

Corollary 0.0.44 (Wilson's theorem)**.** *An integer n is prime if and only if $(n-1)! \equiv -1 \ mod \ n$.*

Theorem 0.0.45. *Let p be an odd prime. Then the quadratic congruence $x^2 + 1 \equiv 0 \ mod \ p$ has a solution if and only if $p \equiv 1 \ mod \ 4$.*

Exercises "TYPE" that you MUST really know how to solve in order to solve the basic part of the midterm.

Of course, it is up to changing the values involved. Of course, more abstract exercise will be asked, and I cannot putt all into a exercise "TYPE". All this exercises are in the class notes or homework. I am not saying the other are not important.

1. Prove using induction on n that 4 divides $1 + 3^{2n+1}$ for all $n \in N$. Do not forget that there is 3 step to follow:
   (a) Initialization, $n = 1$ (depending of where you have to start!)
   (b) Transmission: State induction hypothesis, that is:
   Suppose that the statement is true for SOME ARBITRARY n, and PROVE that the statement is true for n+1 (Be careful! DO NOT forget to use the induction hypothesis).
   (c) Conclusion: By induction, the statement is true for all $n \in \mathbb{N}$.
2. Compute $gcd(24, 36)$. (You might want to use or the extended GCD algorithm, or prime factorization, or direct computation. Depending on how big are the numbers involved.)
3. Compute $lcm(24, 36)$. (You might want to use prime factorization, or direct computation. Depending on how big are the numbers involved.)
4. Prove that 12 and 35 are coprime. (Note that this is the same question as asking: is the fraction 12/35 irreducible, for example) You may use GCD extended algorithm to find that gcd is equal to 1, or direct computation, but also Bezout's theorem (useful when the number are not fixed: remember the exercise of the homework 1: Let $a \in \mathbb{Z}$. Prove that $gcd(2a + 3, a + 2) = 1$ or the one on the class note: Prove that the fraction $(21n + 4)/(14n + 3)$ is irreducible for every natural number n.)
5. Compute the Euclidean division of 100 by 13. (Here I ask you to find the quotient and the remainder) That is $100 = 13 \times 7 + 9$ (i.e. $q = 7$, $r = 9$).

6. Find all the integer solution (or I can ask all the congruence classes solutions mod the GCD of)
$$gcd(2445, 652) = 2445 \times x + 652 \times y$$
(Be careful to answer the question completely, if I ask all the solutions I want them all, if I ask them of the form of congruence classes make sure you give it this way, if I want only one do not loose time in giving me all of them. Also, justify all steps, this is valid for any over exercise, if you use GCD algorithm say you using it, as well as extended GCD algorithm, apply both of them to solve this kind of problem. You can also find a easy particular solution and then you do not need all this, but make sure the solution is clear and not something you found out looking at your classmate exam!). I could also ask: Find all the integer solutions of $56x + 76y = 40$. Then you need to make sure that $gcd(56, 76)|40$ before starting because otherwise there is no solution and then you solve as before. BE CAREFUL, you might have a multiple of the GCD, so you might want to multiply by something after doing the extending GCD algorithm. (See how we did it in class).
7. I can also ask something more abstract like: If a positive integer m is not a perfect square, then $\sqrt{m}$ is irrational or There are infinitely many primes or some question of the Quiz. For this you need to practice that all, there is no miracle if you want to have some intuition or reflexes.
8. Is 97 a prime? (See class note)
9. You must know how to do this exercise type for arithmetic function: Let $g(n)$ be the arithmetic function whose summary function is $f(n) = \sum_{d|n} g(n) = \frac{n-1}{n+1}$. Find $g(24)$. (Here you just have to use the Möbius inversion to find g, and so know how to compute a convolution product. But this is easier than you think, trust me. Think about it you will see.)
(I could also ask something like this: Define the arithmetic function Λ by:
$$\Lambda(n) = \begin{cases} log(p) & n = p^k \\ 0 & \text{otherwise} \end{cases}$$

Show that $\sum_{d|n} \Lambda(d) = log(n)$ whenever n is a positive integer. (Here I just want to see if you understand a definition and you know how to read a sign sum and compute it).

10. Calculate the least non-negative (absolute) residue of 28×33 mod 35. (see class notes)
11. Prove that $a(a+1)(2a+1)$ is divisible by 6 for every integer a. (see class notes)
12. Solve the congruence

$$10x \equiv 6 \ mod \ (12)$$

(I might ask you to give the solution in congruence class form, do not forget to check that $gcd(10,12)|6$ and then you have plenty of way to find a particular solution, and then apply the class theorem to say how many congruence classes there is and to give them ALL. You may want to simplify the equation before at the beginning (Be careful to be able to simplify them using:

Lemma 0.0.46. *(a) Let m divide a, b and n, and let $a' = a/m$, $b' = b/m$ and $n' = n/m$, then*

$$ax \equiv b \ mod \ (n) \ \textit{if and only if} \ a'x \equiv b' \ mod \ (n')$$

(b) Let a and n be coprime, let m divide a and b, let $a' = a/m$ and $b' = b/m$; then

$$ax \equiv b \ mod \ (n) \ \textit{if and only if} \ a'x \equiv b' \ mod \ (n)$$

13. Solve the following simultaneous congruences:

$$x \equiv 2 \ mod \ (3), \ x \equiv 3 \ mod \ (5), \ x \equiv 2 \ mod \ (7)$$

(Do not forget to verify the condition of CRT, and to say when you use it.) I may ask this kind of question as: Consider the simultaneous congruences

$$7x \equiv 3 \ mod \ (12), \ 10x \equiv 6 \ mod \ (14)$$

(you might then need to do 1. first to go to a simpler form) or also I could ask: Consider the linear congruence

$$13x \equiv 71 \ mod \ (380)$$

ANYWAYS, we have seen plenty of ways to solve this equations (see the notes, and choose the quicker one, do not forget to say when you using CRT and to explain your method).

14. Find 2^{68} *mod* 19. (use Little's Fermat theorem) or I could ask Prove that $a^{25} - a$ is divisible by 30 for every integer a. (Be careful or use Corollary or SEPARATE cases because in order to use little's Fermat theorem you need that $a \not\equiv 0$ *mod* p.)

15. Find all the roots of the congruence

$$x^{17} + 6x^{14} + 2x^5 + 1 \equiv 0 \ smod\ 5$$

(Use Little's Fermat theorem more precisely its corollary because You must have all the conditions in order to apply it satisfied.)

Advice to overcome the level of abstraction of this class.

Practice!

The only way to do math is to practice as well as to do sport. Did you ever see a athlete being good just by learning about the theory of the sport he want to be good at ? I have never. For the exact same reason, you will never do math just know the theory, the muscle you are stimulating is your brain. So my main advice is to do all the examples, proofs, homework of the class by your self (even more than once). You might need first to be helped by the answer I gave with. But, at some point you have to be able to pick an exercise/example without the solution, sit without anything else and do it in a quick amount of time. So, also, take time to do your homework seriously, it is better to do half perfectly and understood than all completely badly and in a rush. At some point, you need to write a proof with your own words. If you are lost, mimic the examples of the class notes for a start and when you get it, you will be wanting to try it without the solution.

Overcome the step one by one!

Here, the step that you need to overcome one by one, (you cannot miss a step) in order to do mathematics:

1. Know how to apply result, compute (for example what you do in calculus)
2. Understand new concepts
3. Understand the proof of the result that you know how to apply or example given in class.
4. Be able to reconstruct a proof, example, that you have seem, using logic knowing the main ideas of it.
5. Construct a proof to answer to an exercises using ideas that arise from the proof, examples that have been given to you in class.
6. Make your proof as concise and precise as possible and take the quicker rout to answer the question. The quicker rout does not mean using a very strong theorem to prove a trivial statement. If you use a theorem in some sense you use also its proof and then your proof is longer if the proof of your theorem is long. The length of your proof depends on the length of the theorem you use.
7. Create new concept, new conjecture, new techniques, new mathematics (this is for researchers).

I am here to give you a panel of idea that you can use, then it is you who need to practice to be able to understand when they can be used and will permit you to reach the answer. It is not easy and it takes time.

Change your expectation!

I do not know what you except of a teacher. I think if you except that everything at the end of the course seems easy and clear and that you have to do nothing at home to understand, in my opinion, it is not the right thing to except. And if I did this, I will make you robots that are only able to reproduce a single one thing. I think I would be lying to you to tell you that mathematics is very easy. As any other discipline it takes practice and even more than most of them. The main point of my work I guess is to make you able to work in perfect autonomy and leave some liberty to your mind to think maybe in something that I have even not think about. You cannot manage in math by learning by heart. Maybe you have to change your expectation toward what a mathematical class should bring you, other that the concepts I introduce to your that you could find in any book any notes I could write, and you could read by yourself at home. You need to acquire mathematical intuition that you cannot learn in the book. In order to make you understand this I need you to know the concept from the previous class, then I could stimulate your intuition and logic. If you do not have the tools, we cannot work. If you really want to success and be always up to date, just take a while to review the concept right before the class even just for 30 min, you might progress fact, hopefully it might help you a lot. Everyone is different of course and for some of you everything might be fluid but for most of you, you might win a lot in doing just this.

Methodology! Learn to do a proof!

One thing that I noticed and that you know by now, is that most of you even the best of you have to learn how to organize, write a proof. It is important for any discipline that you learn how to express your idea in a coherent, concise, comprehensible way. You need to learn how to do an induction, a proof by contraposition, a simple direct proof, a proof by contrapositive. But, beside this, how to make yourself perfectly clear.
A general proof steps:

1. Sometimes you might want to work on the different equivalent way that you can retranslate the question, the hypotheses might help you to choose which part of the course will permit you to answer the question, until reaching the point that you get an idea that works and solve the problem QUICKLY (the most important step that you acquire with practice). Here you are almost done if you know how to be clear and organize, and if you have some methodology. Sometimes it is all about righting down a general definition in the context of the exercise, using the appropriated notations.
2. Organize your idea, see if everything is there (all the hypotheses needed) to apply your ideas, sometimes retranslate the theorem, definition that you want to use in the particular case of the exercise.
3. Write down your proof. I want to see, connectors as: We suppose ...., If ..., Then ..., As a consequence, ..., And ...., Or.....,Since..., As .. In order to make your proof smooth and fluid (as a line, that is not broken). But I want also to see what results you are using when you are using it and why you can use it, if you are using a theorem that you have not proven in the line before. Should look like something as: "Since we have $a \not\equiv 0 \ mod \ p$, we can use Fermat's little theorem this give us : .... blablabla.... ", for instance.
4. Reread your proof afterword, please. (While practicing, compare your proof with the notes or ask a friend if he understands it or just leave it alone one day and comeback to it and try to understand yourself after).

Again, you can see a proof as an algorithm that you put into a computer which knows your class material, and is able to reach it only if you tell him what you are using and you have all the hypothesis needed to apply the theorem. Of course, you need to tell him the connexion between them because as everyone knows a computer is stupid. If the computer does not get stuck until the end, and you reach the conclusion. You have a correct proof. If not something is missing. Then you have to make sure that the algorithm is as short as possible keeping in mind that when you call a theorem you need to pass on the computer all its proof. This is a hard thing to do. For now just manage to solve the problem correctly with a right proof in any case you will loose point by itself, penalize yourself, if you use a too long proof during the exam, because you will be loosing time.

During the MIDTERM! Breath, keep calm, THINK and Sometimes be lazy choosing the shorter exit to the solution!

1. **THINK**, do not write down the solution to fast, avoid traps, **THINK!**, but don't be too slow!
2. Take time to read each questions until the end (it might give you ideas on how to solve it) and if needed transform it in an equivalent way that can be more convenient to use.
3. Do not forget to use every hypothesis if they are there there is a reason, tell me when you use each hypothesis to make sure you are not missing one and because it will justify why you are doing what you are doing. Also, if you are missing one most probably your proof has a problem.
4. Think about all the material that you can use related to the question. And try to find the most efficient way to solve it. Having the right idea is the main part of your work, then it is easier.
5. Try to put idea together in a logical way without missing step, in order to finally, write a mathematical proof. DO NOT forget the logical connector (as: if, then, suppose, As a consequence, this is equivalent, if and only if, and, or.....) and make sure they are the right ones to use.
6. If you need to prove that something satisfies a definition you can first write the definition applied to your particular example and then prove each points of the definition. It might be easier to write it down in a draft.
7. Make sure you answered the initial question in the end. Sometimes one looses point just because they stop just before finishing.
8. Reread what you wrote sometimes it is a big mess that even not you I am sure, could even understand. How could I ?
9. Keep in mind that the Midterm that you handle to me it is not a **DRAFT**. I do not want statement all over the pages without logical

connexion between then, like a puzzle that I have to assemble, that will not work at all.

10. Do not write long paragraph trying to convince me that you know how to do, PROVE IT and I will be convince. A proof is a succession of true mathematical statement linked with logical connector. If you are writing a paragraph as you could right it in a english class or literature that is not a proof, you trying to convincing yourself and at the same time me that your "argument" work. Also, a drawing is not a proof, could be part of your draft to help you to think.
11. If it takes plenty of computations and pages to reach the solution, please ask your self isn't it a clever way in order to solve the problem? Using the class notes ?