Sylvain BONNOT

MAT 311 Number Theory

STATE UNIVERSITY OF NEW YORK

We will meet on MWF : 10:40 am to 11:35 am in Physics P112.

First day of class: Monday January 22, 2006.
Final exam : TBA.

Office hours:
every Wedn. from 2:00 pm to 5:00 pm in my office, 5D-148 in the Math Tower.
My office is in the I.M.S (Institute for Math. Sciences), located on floor 5 and a half.

How to contact me?
the best way is to email me there: `bonnot at math dot sunysb dot edu`

Our textbook:
(added monday 01/22): I confirm that our textbook will be the following: *An Introduction to the Theory of Numbers* (Hardcover), Wiley, Fifth edition (January 1991), by Ivan Niven, Herbert S. Zuckerman, Hugh L. Montgomery

Link to Current Homework: The Homework is an important part of this class. I will take it from the book or from other sources. Click here to go to the homework page.

Course notes and announcements:

- The final exam is now graded, and I posted your letter grades on the Solar system, you should be able to view them very soon. You did a rather good job for this final, that was not an easy one! Since I know you want to do some more number theory in the summer, I give you the correction of the final. I wish you good luck for the rest of your exams, and have a great summer!

- NEW! Please try the practice final, and if you are stuck read its correction.

- The correction for HW9 is available.

- Here is a Practice Final that you should try. Ask me questions about it if you need to! The final exam is next week, on Wed.9th, 8am to 10:30am, usual room. It covers everything from the beginning.

- Here is a beginning: some questions . Of course, you will have more on monday, but you already have to finish a HW, I guess?

- I promised you the end of the proof of the fact that a periodic continued fraction corresponds to a quadratic irrational number. Also, the correction for HW8 is on the HW page.

- HW9 is available on the HW page.

- HW8 has been updated: I changed a small error in problem 2, and added some hints for the last problem.
- HW8 is available.
- You might want to check the correction: scan1, scan2,scan3. I don't give any homework for the break: have a well-deserved Springbreak and see you in April!
- Your midterm will be graded during the break, and will be returned on wed. april 11th. If you need your grade earlier, send me an email. The monday class (april 9th) will be given by our grader Caner Koca, about continued fractions. We will use them to describe the invertible elements in quadratic fields.
- About Midterm II I corrected the practice exam this morning: in case you need it, here is the file of the correction. The second midterm exam is this friday, usual room, usual time. Also the correction for HW7 is on the HW page.
- You should try this practice exam.You will have a correction of it on monday. Prepare your questions for me! And remember that the exam is on friday 30th!!
- The correction of HW6 is on the HW page, and HW7 has been posted: please notice that it is a much shorter one, that it is due on monday, and also that you are encouraged to ask questions about it!(you are also encouraged to return it)
- The correction of the midterm and HW5 are available... correction of the midterm Also HW6 is on the HW page.
- Midterm I is graded You did a pretty good job, the average is around 63/100... The next Hw assignment will be given this Friday (03/09).
- Correction for the practice exam If you tried it, you may want to read its correction ...
- Next HW assignment will be given on monday On monday we will review for the exam, so prepare your questions for me! The correction for the practice exam will be here very soon...You can bring your HW5 on monday too.

Midterm I is next week on Wednesday March 7th, usual room, usual time Please read these informations about what you should know for next week.

Brand new practice exam !! Please try this practice midterm 1, and remember that you will have a detailed correction available very soon...

New HW5 is on HW page.

Please read this proof of the Quadratic reciprocity.Ask me questions if you need!

The two midterms have been scheduled, please see below.

The correction for HW3 is available on the HW page.

Here is a new assignment: HW4.

The correction of HW2 is now available.

Here is the third homework assignment: HW3.

Here is the second homework assignment: HW2.

The correction of HW1 is now available.

Here is the first homework assignment: HW1. Don't hesitate to ask me questions if something is not clear for you!

Quick intro: Number theory is certainly one of the oldest subject within mathematics. Already 36 centuries ago in tablets written in Babylone, there were examples of such problems. Some mathematicians like to say that it occupies within mathematics the same place as mathematics within science...Some people like to see it as the purest domain in mathematics, and yet some others like to see all its applications to cryptography, computer science,etc...
Number theory has the remarkable advantage of being able to formulate extremely deep problems almost without prerequisites. A model for this is certainly Fermat's last theorem, that can be stated in one line but that resisted all the efforts of mathematicians for centuries... For this reason, I think it is an excellent "entry point" to mathematics: we will start with very simple material like divisibility properties, congruences, continue with simple Diophantine equations, and slowly progress towards deeper questions like Quadratic reciprocity.
I will not hesitate to provide introductions to much recent material, like one and two-dimensional representations, or even the Absolute Galois group, which is nowadays one of the most mysterious objects of contemporary mathematics, and one that is certainly the center of a tremendous mathematical activity.

Prerequisites:
For this class you need to have taken MAT 312 or 313 or 318.

Link to Current Homework: Regularly you will have to consult this homework page to know what has been assigned.

Syllabus :

Day of	**Sections Covered**
Week 1:January 22,24,26	Divisibility, prime numbers,repartition of primes, rational points on circle
Week 2:Jan. 29,31,Feb. 02	Congruences, Euclid algorithm, linear equations
Week 3:Feb. 5,7,9	Euler's phi function, summary about groups,rings,Chinese remainder theorem
Week 4:February 12,14,16	Structure of the multiplicative group, existence of square roots
Week 5:Feb. 19,21,23	Quadratic reciprocity theorem
Week 6:Feb. 26,28,March 02	The RSA cryptosystem, Rabin's system, basic attacks on RSA
Week 7:March 5,7,9	Review,exam: midterm 1
Week 8:March 12,14,16	Ideals, quotient of a ring by an ideal, quadratic extensions
Week 9:March 19,21,23	Prime ideals (continued), basic intro to topological spaces,Spec of a ring
Week 10:March 26,28,30	Review, midterm II
Week 11:April 9,11,13	Continued fractions and approximations of real numbers
Week 12:April	Intro to elliptic functions and cryptography

16,18,20	

Exams:

Midterm 1	Wed. March 7th	Usual room
Midterm 2	Fr. March 30th	Usual room
Final	Wed May 9,2007, 8:00 am to 10:30 am	Usual room

Homework and grading policy: Here is how your final grade will be computed. of the following:

Exam I	25%
Exam II	25%
Final Exam	35%
Homework	15%

Late homework will not be accepted.

DSS advisory:

If you have a physical, psychological, medical, or learning disability that may affect your course work, please contact Disability Support Services (DSS) office: ECC (Educational Communications Center) Building, room 128, telephone (631) 632-6748/TDD. DSS will determine with you what accommodations are necessary and appropriate. Arrangements should be made early in the semester (before the first exam) so that your needs can be accommodated. All information and documentation of disability is confidential. Students requiring emergency evacuation are encouraged to discuss their needs with their professors and DSS. For procedures and information, go to the following web site http://www.ehs.sunysb.edu and search Fire safety and Evacuation and Disabilities.

MAT 311 Homework Assignments

Fall 2006

Link to main page for MAT 311.
Mathematics department

#	Problems	Due Date
1	**HW1** Complete correction: correctionHW1	**Friday** 02/02/2007
2	**HW2** Complete correction: correctionHW2	**Friday** 02/09/2007
3	**HW3** Complete correction: correctionHW3	**Friday** 02/16/2007
4	**HW4** Complete correction: correctionHW4	**Friday** 02/23/2007
5	**HW5** Complete correction: correctionHW5	**Friday** 03/02/2007
6	**HW6** Complete correction: correctionHW6	**Monday** 03/19/2007
7	**HW7** Complete correction: correctionHW7	**Monday** 03/26/2007
8	**HW8** Complete correction: correctionHW8	**Wed.** 04/18/2007
9	**HW9** Complete correction: correctionHW9	**Fr.** 04/27/2007

MAT 311 05/09/2007

Correction of Final Exam

Name:

Student I.D:

Problem 1. (30 points)

1. How many solutions $(x,y)\in\mathbb{Z}\times\mathbb{Z}$ does have the equation: $4x^2+3y^2=1$?
2. How many solutions $(x,y)\in\mathbb{Z}\times\mathbb{Z}$ does have the equation: $2x^2-3y^2=1$?
3. How many solutions $(x,y,z)\in\mathbb{Z}^3$ does have the equation: $x^2+y^2=4z+3$?

Correction:

1. No solution: Because $(x,y)\neq(0,0)$ implies $4x^2+3y^2\geqslant 3>1$.
2. No solution: in $\mathbb{Z}/3\mathbb{Z}$, the only possible values for $2x^2$ are 0, 2 so $2x^2-3y^2$ which is congruent to $2x^2$
   modulo 3 cannot be congruent to 1.
3. No solution: by working modulo 4, one realizes that the only possible values for x^2+y^2
   modulo 4 are 0,1,2, and not 3.

Problem 2. (35 points) An elliptic curve with no integer points

In this problem we want to show that the curve E: $y^2=x^3+7$ has no points (x,y) with coordinates in $\mathbb{Z}^2$.

1. Suppose that (x,y) is a solution in integers. Show that x must be odd.
2. Show that $y^2+1=(x+2).(x^2-2x+4)$.
3. Show that x^2-2x+4 must be congruent to 3 modulo 4.Explain why x^2-2x+4 must be divisible by some prime q satisfying $q\equiv 3\ (\bmod 4)$.
4. Reduce the original equation modulo q and deduce from it that (-1) must have a square root in $\mathbb{Z}/q\mathbb{Z}$. Show that this is impossible, thus proving that the equation has no solutions in integers.

Correction:

1. If x is even then y^2 would be of the form $8k+7$, but by writing them down, one sees that squares of integers can only be congruent to 0,1,4 modulo 8.Thus x is odd.
2. Just expand the product.
3. We proved that x is odd $=2k+1$, thus $x^2-2x+4=(2k+1)(2k-1)+4\equiv 4k^2+3$ must be congruent to 3 mod 4. Now the prime numbers dividing x^2-2x+4 cannot be all of type $4k+1$(because the product of their powers would be of same type, which is not the case).
4. Since q divides x^2-2x+4, it must divide y^2+1, which means that y would be a square root of -1 mod q. Since $(-1)^{\frac{q-1}{2}}=-1$, this is a contradiction.

Problem 3. (20 points) Let p be an odd prime such that $p = 8n + 1$ for some integer n.We have seen in class that the non-zero elements of $\mathbb{Z}/p\mathbb{Z}$ form a group for the multiplication law, and that this group is cyclic of order $p - 1 = 8n$. We consider one generator, called r, of this multiplicative group $(\mathbb{Z}/p\mathbb{Z} - \{0\}, \times)$.

Show that the solutions of the congruence $x^2 \equiv 2 \pmod p$ are given by

$$x \equiv \pm (r^{7n} + r^n)(\bmod p)$$

Correction:

Since $\mathbb{Z}/p\mathbb{Z}$ is a field, there are at most 2 solutions for the polynomial equations, so if the proposed numbers are solutions, they will constitute the complete set of solutions.

Let's set $x = (r^{7n} + r^n)$. Then $x^2 = (r^{7n} + r^n)^2 = r^{14n} + 2r^{8n} + r^{2n} = r^{6n} + 2 + r^{2n} = 2 + r^{2n}(1 + r^{4n})$, because $r^{8n} = 1$. For the same reason, one must have $r^{4n} = -1$, which implies the conclusion.

Problem 4. (45 points)

Let p be an odd prime. We want to show the following: $p \equiv 1, 3 (\bmod 8)$ if and only if p can be written as $p = x^2 + 2y^2$ for some choice of integers x and y. For the rest of the problem, you can use (without proving it) the following result coming from quadratic reciprocity:
if $p \equiv 1, 3 (\bmod 8)$ then there exists an integer r such that $r^2 \equiv -2$ modulo p.

1. Show that if $p = x^2 + 2y^2$ for some integers x and y, then p is not congruent to 5, nor 7 modulo 8. (Hint: what are the possible values modulo 8 taken by squares of integers?) Conclude that necessarily p must be congruent to 1 or 3 in this case.

2. Show the following lemma (independent of the rest of the problem):
   Lemma. If $x \in \mathbb{R}$, $n \in \mathbb{N}$, then there exists a fraction $\frac{a}{b}$ in lowest terms such that $0 < b \leqslant n$ and
   $$\left| x - \frac{a}{b} \right| \leqslant \frac{1}{b(n+1)}.$$
   (**Hint**: approximation by continued fractions...)

3. Apply the lemma to $x = \frac{-r}{p}$ (where r is a square root of (-2) in $\mathbb{Z}/p\mathbb{Z}$), and $n = \lfloor \sqrt{p} \rfloor$(this means the integer part of $\sqrt{p}$). Letting $c = r.b + p.a$, show the following:
   a) $c^2 + 2b^2 \equiv 0$ modulo p.
   b) $0 < c^2 + 2b^2 < 3p$.
   c) Both cases $c^2 + 2b^2 = 2.p$ and $c^2 + 2b^2 = p$ give a solution to the initial problem.

4. Conclude.

Correction:

1. Squares of integers modulo 8 can only take the values 0,1,4, therefore $2y^2$ can only take the values 0,2 modulo 8, and the sum $x^2 + 2y^2$ can only take the values 0,1,2,3,4,6, but not 5,7. Thus the odd prime p must be congruent to 1 or 3 modulo 8.

2. From the theory of continued fractions, we know the existence of approximations
   $$\left| x - \frac{p_i}{q_i} \right| \leqslant \frac{1}{q_i . q_{i+1}},$$

where the q_i form an unbounded increasing sequence of integers.Thus for any integer $n+1$, there exists an integer i such that $q_i < n+1 \leqslant q_{i+1}$, and this implies the result because $1/q_{i+1} \leqslant 1/(n+1)$ and at the same time $0 < q_i \leqslant n$.

3.

   a) First one has $c^2 \equiv r^2.b^2 \equiv -2b^2$ mod p, hence the result.

   b) Now one has $\left|\frac{a.p+b.r}{p.b}\right| = \left|\frac{-r}{p} - \frac{a}{b}\right| \leqslant \frac{1}{b(n+1)}$, so $c^2 \leqslant \frac{p^2}{(n+1)^2} < p$.

   Moreover one has $b \leqslant n \leqslant \sqrt{p}$, so $2b^2 \leqslant 2p$. Putting everything together, one gets the desired inequality.

   c) The quantity $c^2 + 2b^2$ must be a multiple of p, strictly between 0 and $3p$, so it can be p or $2p$. If it is p then we are done.

   Suppose it is now equal to 2p, then this would imply that c^2 is even, so c itself would be even equal to $2d$, but then our equation would become $4d^2 + 2b^2 = 2.p$ which implies $2d^2 + b^2 = p$, a solution to our problem.

4. If p is congruent to 1 or 3 modulo 8, then we can find a solution in integers to the equation $p = x^2 + 2y^2$, and these two conditions are equivalent.

Problem 5. (40 points)

1. Show that the ring of Gaussian integers $\mathbb{Z}[i]$ is isomorphic to $\mathbb{Z}[X]/I$, where I is the ideal generated by X^2+1.
2. Find an explicit isomorphism between $\mathbb{Z}[X]/(X-3)$ and $\mathbb{Z}$.
3. Is the ring $\mathbb{Z}[X]/(3X-1)$ isomorphic to $\mathbb{Z}$?
4. Show that if $\varepsilon \in \mathbb{Z}[i]$ has an inverse in $\mathbb{Z}[i]$ (we call such an element a *unit* of $\mathbb{Z}[i]$) then necessarily $\varepsilon^5 = \varepsilon$.(Hint: use the norm $N(a+b.i) = a^2+b^2$ and its properties).
5. Show that $\mathbb{Q}[X]/(X^2+X+1)$ is a field and find the inverse of the element
   $X+2$ (mod X^2+X+1).

Correction:

1. Consider the ring morphism

$$\begin{array}{rccc} \varphi\colon & \mathbb{Z}[X] & \longrightarrow & \mathbb{Z}[i] \\ & P(X) & \longmapsto & P(i) \end{array}$$

   This is clearly surjective ($a + b.i$ can be obtained as $\varphi(a + b.X)$). The kernel contains (X^2+1). Moreover, if one writes the euclidean division of $P(X)$ by X^2+1, one obtains a remainder of degree 1, $a + b.X$, which is zero if and only if $a + b.i = \varphi(P(X))$ is zero, so the kernel is the ideal (X^2+1).One concludes with the isomorphism theorem.

2. Just consider

$$\begin{array}{rccc} \varphi\colon & \mathbb{Z}[X] & \longrightarrow & \mathbb{Z} \\ & P(X) & \longmapsto & P(3) \end{array}$$

   This is surjective of kernel $(X-3)$, hence the result.

3. Let's consider $\bar{X}$ (or if you prefer X mod $(3X-1)$) in $\mathbb{Z}[X]/(3X-1)$. It's an element that has the property that $3.\bar{X} = 1$, so 3 is invertible in that ring.Now in $\mathbb{Z}$, we know that 3 is not invertible, therefore the two rings cannot be isomorphic.

4. Invertible elements in $\mathbb{Z}[i]$ are the elements with norm=1. It's easy to check that only the 4th roots of unity are invertible, and they satisfy the required equation.

5. The polynomial is irreducible (roots are j, j^2), so we get a field. Now $(X+2)(X-1) \equiv -3$ so the inverse of $X+2$ is $(-1/3)(X-1)$.

Problem 6. (30 points)

1. Find the solutions $(x, y) \in \mathbb{Z}^2$ to the equation $7x - 12y = 4$.
2. Find the continued fraction expansion of $\frac{41}{15}$.

Correction:

1. You'll find $x = 4 + 12k$, $y = 2 + 7k$, where k is an arbitrary integer.
2. You get $41/15 = [2; 1, 2, 1, 3]$

Problem 1. *The curve*

$$y^2 = x^3 + 8$$

contains the point $(1, -3)$ *and* $(-7/4, 13/8)$. *The line through these two points intersects the curve in exactly one other point. Find it and explain why its coordinates are rational numbers.*

Answer. The equation of the line joigning the 2 points is given by : $\frac{y+3}{x-1} = \frac{13/8+3}{-7/4-1} = -\frac{37}{22}$, so it is $y = -\frac{37}{22}x - \frac{25}{22}$. Plug this into the equation of the curve:

$$x^3 + 8 = (-\frac{37}{22}x - \frac{25}{22})^2.$$

This is a cubic equation $x^3 + ax^2 + bx + c$. Since we know already three roots, we know that there is a third one. Moreover, the sum of the three roots must be $(-a) = (37/22)^2 = 1369/484$.Because of this property we know that the third root α must be a rational number (it's a sum of rational numbers). Thus $1 + (-7/4) + \alpha = 1369/484$.So $\alpha = 1732/484$. Plug this into the equation of the line to find the y coordinate.

Problem 2. *Solve* $x^{39} \equiv 3$ *(mod 13)* .

Answer. By Fermat's theorem, you know that $x^{12} \equiv 1$ modulo 13.Therefore $x^{39} \equiv x^{36}.x^3 \equiv x^3$, and we are reduced to the resolution of $x^3 \equiv 3$ modulo 13. You can do it by hand and realize that there is no solution.

Problem 3. *Find all integers n such that* $\phi(n) = n/6$.*(Remember that* $\phi(n)$ *is the number of integers k such that* $1 \leq k \leq n$ *and* $GCD(k, n) = 1$*).*

Answer. Use the formula we had: $\phi(n) = n.(1 - 1/p_1) \ldots (1 - 1/p_k)$, where the p_i are the prime factors appearing in the decomposition of n. Thus we must have $1/6 = (1 - 1/p_1) \ldots (1 - 1/p_k)$. Because of the denominator 6, both prime factors 2,3 must appear. But then $(1 - 1/2).(1 - 1/3) = 1/2$.And among all the other possible factors $(1 - 1/p_i)$, none of them can produce a denominator multiple of 3, therefore the equation has no solution.

Problem 4. *Let* $d_1, \ldots, d_r$ *be the numbers dividing n, including* 1 *and n. The* t^{th} power sigma function $\sigma_t(n)$ *is equal to the sum of the* t^{th} *powers of the divisors of n,*

$$\sigma_t(n) = d_1^t + \ldots + d_r^t.$$

For example, $\sigma_2(10) = 1^2 + 2^2 + 5^2 + 10^2 = 130$.

1. *Compute the values of* $\sigma_3(10), \sigma_0(18)$.

2. *Show that if* $GCD(m, n) = 1$, *then* $\sigma_t(mn) = \sigma_t(m)\sigma_t(n)$.

Answer. 1. $\sigma_3(10) = 1^3 + 2^3 + 5^3 + 10^3 = 1134, \sigma_0(18) = 1+1+1+1+1+1 = 6.$

2. $GCD(m,n) = 1$, then $\sigma_t(mn) = \sigma_t(m)\sigma_t(n)$.

   When m, n are coprime, we proved in the first midterm that there is a bijection between the set of divisors of mn and the set of ordered pairs (d, d'), where d is a divisor of m, and d' is a divisor of n (the correspondance being given by $(d, d') \mapsto d.d'$). Now if we expand the product $\sigma_t(m)\sigma_t(n)$, we get a sum over all the ordered pairs (d, d') (d divisor of m, d′ divisor of n), of the t^{th} power of $(d.d')$. By the remark above, we then get the sum of the t^{th} powers of all the divisors of mn, and this is $\sigma_t(mn)$.

Problem 5. *Suppose that a has a square root in $\mathbb{Z}/p\mathbb{Z}$, for p prime, and suppose further that $p \equiv 5$ (mod 8) .*

Show that one of the values $x = a^{p+3}/8$ or $x = (2a).(4a)^{(p-5)/8}$ is a solution to the congruence $x^2 \equiv a$ (mod p) .

Answer. We know that a has a square root, therefore necessarily one has $a^{(p-1)/2} = 1$. Observe that $p = 8k + 5$ implies $p - 1$ is a multiple of 4. Now there are two cases:

1. First case: $a^{\frac{p-1}{4}} = +1$, but then, by multiplying by a both sides one gets: $a^{\frac{p+3}{4}} = +a$. But since $p+3$ is a multiple of 8, one can consider $x = a^{\frac{p+3}{8}}$ and this will be a square root of a.

2. Second case: $a^{\frac{p-1}{4}} = -1$.But then $a.x^2 = ((2a).(4a)^{(p-5)/8})^2 = a^2.4^{(p-1)/4}.a^{(p-1)/4} = a^2.(-1).(2^{(p-1)/2})$. In the proof of the quadratic reciprocity, we proved that when $p \equiv 5$ (mod 8) we have $2^{(p-1)/2} = -1$, therefore we have $a.x^2 = a^2$, and then x is a square root of a.

Problem 6. 1. *If N is not a perfect square, find a specific value for K so that the inequality $K/b^2 < |a/b - \sqrt{N}|$ holds for every rational number a/b. The value of K will depend on N but not on a or b.)*

2. *Use the above result to find all rational numbers a/b satisfying $|a/b - \sqrt{7}| \leq 1/b^3$.*

Answer. Consider the quadratic polynomial $f(X) = X^2 - N$. Then on the interval $[0, 2\sqrt{N}]$, one has $|f'(x)| = |2x| \leq 4\sqrt{N}$, so one gets $\frac{1}{b^2} < |f(a/b) - f(\sqrt{N})| \leq 4\sqrt{N}.|\frac{a}{b} - \sqrt{N}|$.Now if a/b is larger than $2\sqrt{N}$, then $|\frac{a}{b} - \sqrt{N}| \geq \sqrt{N}$ which is larger than $1/(4\sqrt{N}.b^2)$, so our lower bound works in every case.

Suppose now that you have, $|a/b - \sqrt{7}| \leq 1/b^3$, then you would deduce $K/b^2 \leq 1/b^3$, and therefore $\frac{1}{4\sqrt{7}} < \frac{1}{b}$, so $b < 4\sqrt{7}$, and then $b < 11$, so $b \leq 10$.Now we can try by hand the possible fractions: we find that the only possible solutions are $a/b = 3/1$, and $a/b = 8/3$.

Problem 7. *Let p be a prime number such that $p \equiv 1 \pmod{4}$, and assume that $u^2 \equiv -1 \pmod{p}$. Write u/p as a continued fraction $[a_0, a_1, \ldots a_n]$, and let i be the largest integer such that $q_i \leq \sqrt{p}$ (remember that the q_i are the denominators of the continued fractions $[a_0, \ldots, a_i]$)*

1. *Show that $|p_i/q_i - u/p| < 1/(q_i\sqrt{p})$ and hence that $|p_i p - uq_i| < \sqrt{p}$.*

2. *Put $x = q_i, y = p_i p - uq_i$. Show that $0 < x^2 + y^2 < 2p$, and that $x^2 + y^2 \equiv 0 \pmod{p}$ .Deduce that $x^2 + y^2 = p$.*

Answer.

1. First, we know from the theory of continued fractions that $|p_i/q_i - u/p| \leq 1/(q_i q_{i+1})$ but this implies the result, because necessarily one has $q_{i+1} > \sqrt{p}$ (by definition of q_i).Multiply by the denominators to get the other identity.

2. One has $0 < x^2 + y^2 < q_i^2 + p \leq 2p$. Now $x^2 + y^2 = q_i^2 + (p_i p - uq_i)^2 \equiv q_i^2(1 + u^2) \equiv 0$ (mod p) .And now the conclusion comes from the fact that p is the only multiple of p strictly between 0 and p.

Problem 8. *Prove that $11 + 2\sqrt{6}$ is a prime in $\mathbb{Q}(\sqrt{6})$.(We recall that a prime in a quadratic number field $\mathbb{Q}(\sqrt{m})$ is an element α that is divisible only by invertible elements, and by elements that are products of α by some invertible element).*

Answer. As seen before, we use the Norm map, where $N(a + b\sqrt{6}) = a^2 - 6b^2$. The invertible elements in $\mathbb{Q}(\sqrt{6})$ are the one with norm equal to ±1. Since $N(11 + 2\sqrt{6}) = 121 - 6.4 = 97$ is prime, so is $11 + 2\sqrt{6}$ (otherwise one could write $11 + 2\sqrt{6}$ as a product $(a + b\sqrt{6}).(c + d\sqrt{6})$ with norms different from ± 1).

Math 311 **Practice Final**

Problem 1. *The curve*

$$y^2 = x^3 + 8$$

contains the point $(1, -3)$ *and* $(-7/4, 13/8)$. *The line through these two points intersects the curve in exactly one other point. Find it and explain why its coordinates are rational numbers.*

Problem 2. *Solve* $x^{39} \equiv 3$ *(mod 13)* .

Problem 3. *Find all integers n such that* $\phi(n) = n/6$.*(Remember that* $\phi(n)$ *is the number of integers k such that* $1 \leq k \leq n$ *and* $GCD(k, n) = 1$*).*

Problem 4. *Let* $d_1, \ldots, d_r$ *be the numbers dividing n, including* 1 *and n. The* t^{th} power sigma function $\sigma_t(n)$ *is equal to the sum of the* t^{th} *powers of the divisors of n,*

$$\sigma_t(n) = d_1^t + \ldots + d_r^t.$$

For example, $\sigma_2(10) = 1^2 + 2^2 + 5^2 + 10^2 = 130$.

1. *Compute the values of* $\sigma_3(10), \sigma_0(18)$.

2. *Show that if* $GCD(m, n) = 1$, *then* $\sigma_t(mn) = \sigma_t(m)\sigma_t(n)$.

Problem 5. *Suppose that a has a square root in* $\mathbb{Z}/p\mathbb{Z}$, *for p prime, and suppose further that* $p \equiv 5$ *(mod 8)* .

Show that one of the values $x = a^{p+3}/8$ *or* $x = (2a).(4a)^{(p-5)/8}$ *is a solution to the congruence* $x^2 \equiv a$ *(mod p)* .

Problem 6.

1. *If N is not a perfect square, find a specific value for K so that the inequality* $K/b^2 < |a/b - \sqrt{N}|$ *holds for every rational number a/b. The value of K will depend on N but not on a or b.)*

2. *Use the above result to find all rational numbers a/b satisfying* $|a/b - \sqrt{7}| \leq 1/b^3$.

Problem 7. *Let p be a prime number such that* $p \equiv 1$ *(mod 4)* , *and assume that* $u^2 \equiv -1$ *(mod p)* . *Write u/p as a continued fraction* $[a_0, a_1, \ldots a_n]$, *and let i be the largest integer such that* $q_i \leq \sqrt{p}$ *(remember that the* q_i *are the denominators of the continued fractions* $[a_0, \ldots, a_i]$*)*

1. *Show that* $|p_i/q_i - u/p| < 1/(q_i\sqrt{p})$ *and hence that* $|p_i p - u q_i| < \sqrt{p}$.

2. *Put* $x = q_i, y = p_i p - u q_i$. *Show that* $0 < x^2 + y^2 < 2p$, *and that* $x^2 + y^2 \equiv 0$ *(mod p)* .*Deduce that* $x^2 + y^2 = p$.

Problem 8. *Prove that* $11 + 2\sqrt{6}$ *is a prime in* $\mathbb{Q}(\sqrt{6})$.*(We recall that a prime in a quadratic number field* $\mathbb{Q}(\sqrt{m})$ *is an element* α *that is divisible only by invertible elements, and by elements that are products of* α *by some invertible element).*

I suggest that for monday you finish the HW, and that you try these 3 questions. On monday, you will have online a full practice final... Read the corrections of the midterms, HWs and make sure to prepare questions for me during the week!

Problem 1. *Solve the congruence* $x^2 + x + 7 \equiv 0$ *(mod 27) .*

Problem 2. *If* p *is an odd prime, how many solutions are there to* $x^{p-1} \equiv 2$ *(mod* p*) ?*

Problem 3. *Prove that if* $a^3 \equiv 1$ *modulo a prime* p*, then* $1 + a + a^2 \equiv 0$ *modulo* p*, and* $(1 + a)^6 \equiv 1$ *modulo* p*.*

More problems are on the way...

Math 311 Notes on continued fractions

I would like to finish the proof of the following (we already proved the "if" statement):

Theorem. *A number $\alpha \in \mathbb{R} - \mathbb{Q}$ is quadratic irrational if and only if its continued fraction expansion is eventually periodic.*

Proof of the theorem, taken from Hardy-Wright.

Lemma. *If* $\alpha = a_0 + \frac{1}{a_1 + \frac{1}{\ldots + \frac{1}{a_{n-1}+\alpha_n}}}$, *then one has* $\alpha = \frac{\alpha_n p_{n-1} + p_{n-2}}{\alpha_n q_{n-1} + q_{n-2}}$.

This is not too difficult to prove (a proof by induction works: see the book if you need help).

Assume now that α is a root of an irreducible polynomial $P(X) = aX^2 + bX + c$ with integer coefficients. After substituting the value for α, one gets that

$$A_n \alpha_n^2 + B_n \alpha_n + C_n = 0$$

with explicit formulas $A_n = ap_{n-1}^2 + bp_{n-1}q_{n-1} + cq_{n-1}^2$, $B_n = 2ap_{n-1}p_{n-2} + b(p_{n-1}q_{n-2} + p_{n-2}q_{n-1}) + 2cq_{n-1}q_{n-2}$, and also $C_n = ap_{n-2}^2 + bp_{n-2}q_{n-2} + cq_{n-2}^2$.

Notice that $A_n \neq 0$ (otherwise p_{n-2}/q_{n-2} would be a root of $P(X)$). Also notice the following:

$$B_n^2 - 4A_nC_n = (b^2 - 4ac).(p_{n-1}q_{n-2} - p_{n-2}q_{n-1}) = \pm(b^2 - 4ac).$$

Now you need to remember that we had proven in class that $\alpha = \frac{p_{n-1}}{q_{n-1}} + \frac{x_{n-1}}{q_{n-1}}$, with $|x_{n-1}| < 1/q_{n-1}$ and thus $p_{n-1} = q_{n-1}\alpha + x_{n-1}$.

Therefore,

$$A_n = a(q_{n-1}\alpha + x_{n-1})^2 + bq_{n-1}(q_{n-1}\alpha + x_{n-1}) + cq_{n-1}^2,$$

but this is also

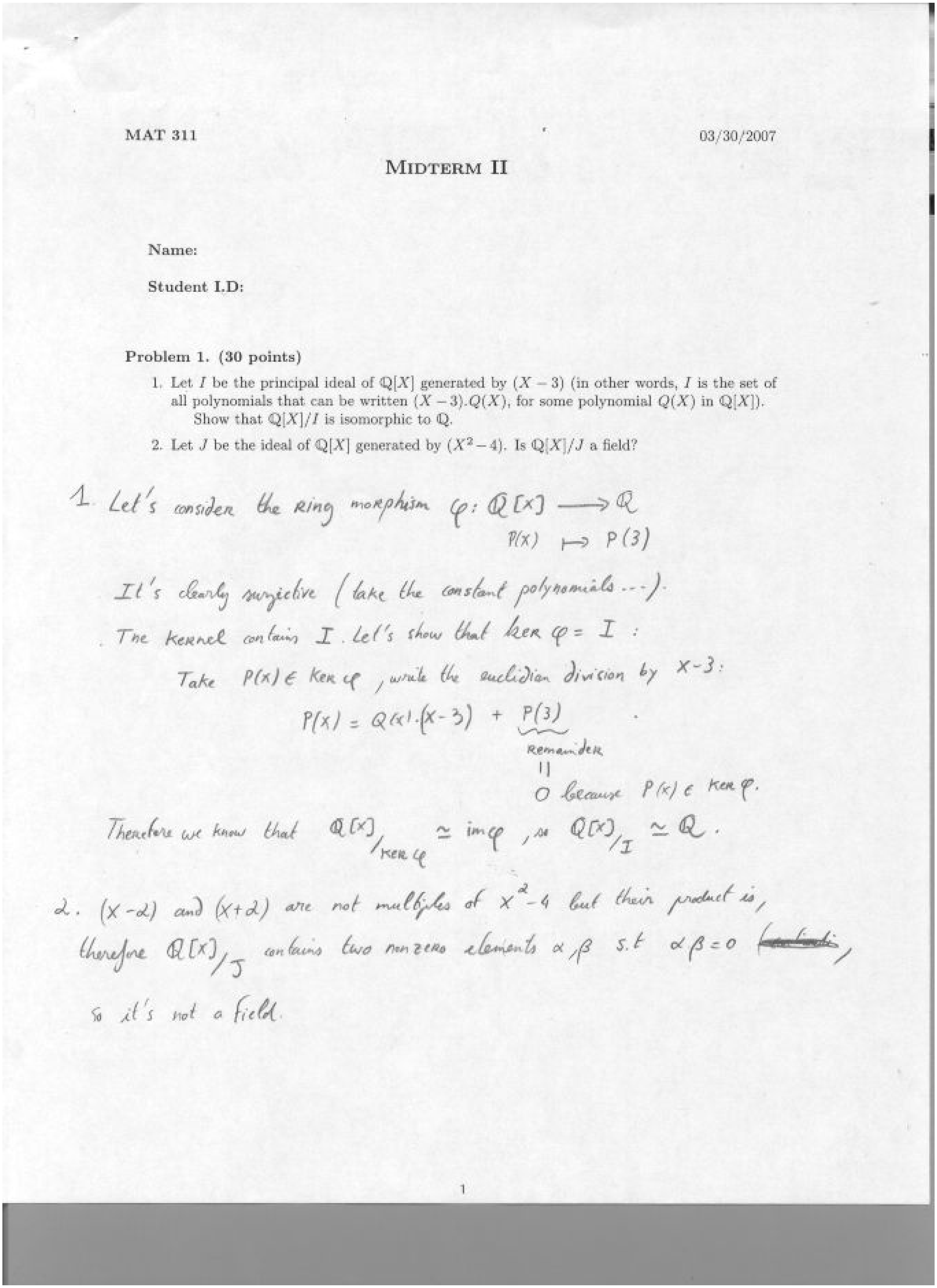
$$A_n = (a\alpha^2 + b\alpha + c)q_{n-1}^2 + 2a\alpha x_{n-1}.q_{n-1} + ax_{n-1}^2 + bx_{n-1}.q_{n-1}$$

, and since α is a root of $P(X)$, one gets

$$A_n = 2a\alpha x_{n-1}.q_{n-1} + ax_{n-1}^2 + bx_{n-1}.q_{n-1},$$

which implies $|A_n| < 2|a\alpha| + |a| + |b|$. Now $C_n = A_{n-1}$, so the same estimate holds. Using the relation on the discriminant, one gets also $B_n^2 \leq 4|A_nC_n| + |b^2 - 4ac| \leq 4(2|a\alpha| + |a| + |b|)^2 + |b^2 - 4ac|$.

All these upper bounds do not depend on n, therefore there is only a finite possible number of values for A_n, B_n, C_n.Thus one can find a triple (A, B, C) of values that is taken three times, for $\alpha_{n_1}, \alpha_{n_2}, \alpha_{n_3}$. Thus one has three roots of the same quadratic polynomial $AX^2 + BX + C$, therefore two of them must be equal, say $\alpha_{n_1} = \alpha_{n_2}$. Thus the integers in the expansion must satisfy $a_{n_1} = a_{n_2}, a_{n_1+1} = a_{n_2+1}, \ldots$ □



MAT 311 03/30/2007

Midterm II

Name:

Student I.D:

Problem 1. (30 points)

1. Let I be the principal ideal of $\mathbb{Q}[X]$ generated by $(X-3)$ (in other words, I is the set of all polynomials that can be written $(X-3).Q(X)$, for some polynomial $Q(X)$ in $\mathbb{Q}[X]$). Show that $\mathbb{Q}[X]/I$ is isomorphic to $\mathbb{Q}$.
2. Let J be the ideal of $\mathbb{Q}[X]$ generated by (X^2-4). Is $\mathbb{Q}[X]/J$ a field?

1. Let's consider the ring morphism $\varphi : \mathbb{Q}[X] \longrightarrow \mathbb{Q}$

$$P(X) \longmapsto P(3)$$

It's clearly surjective (take the constant polynomials ...).

. The kernel contains I. Let's show that $\ker\varphi = I$:

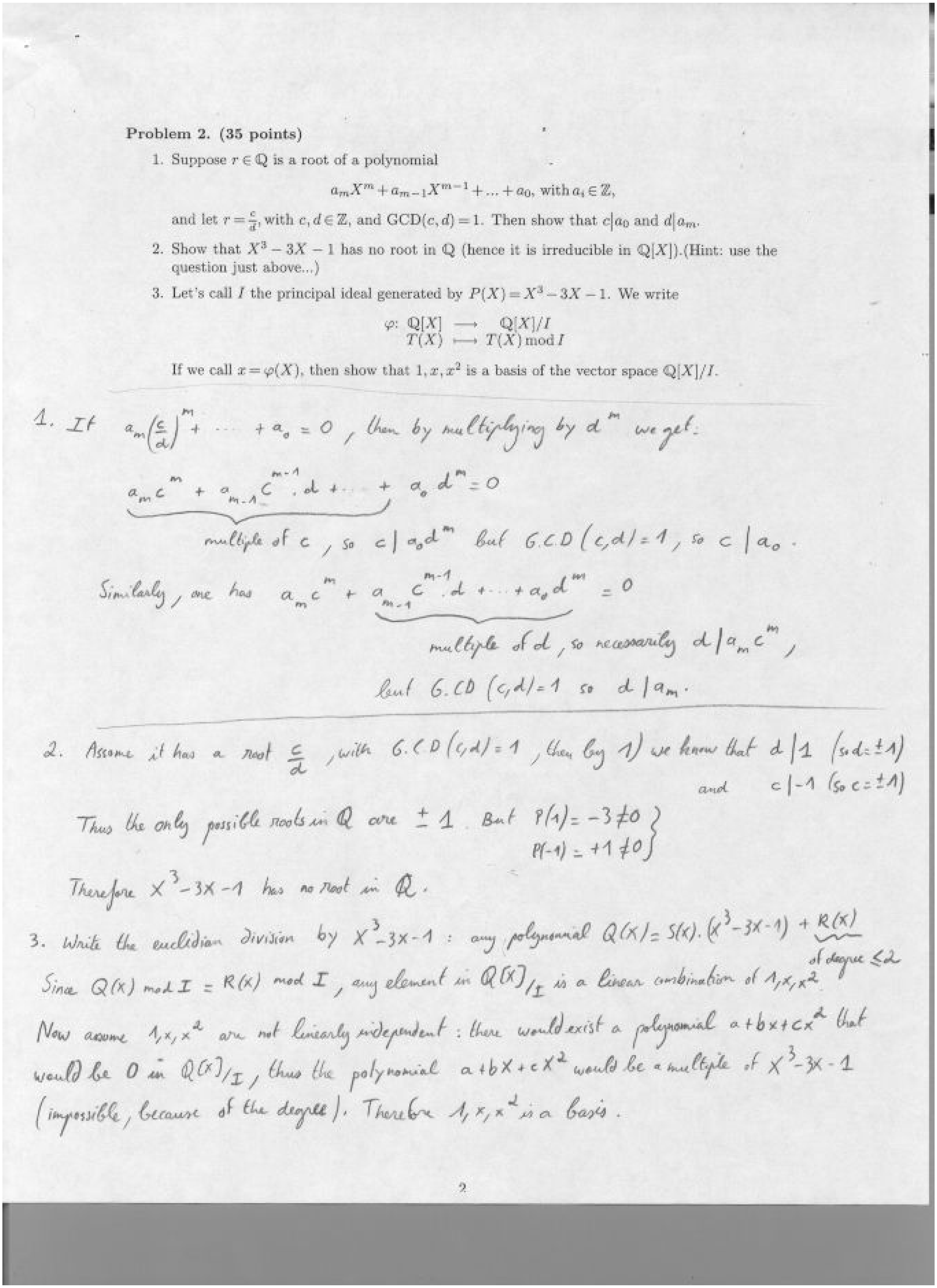
Take $P(X) \in \ker\varphi$, write the euclidian division by $X-3$:

$$P(X) = Q(X).(X-3) + \underbrace{P(3)}_{\substack{\text{Remainder} \\ \shortparallel \\ 0 \text{ because } P(X) \in \ker\varphi}} .$$

Therefore we know that $\mathbb{Q}[X]/_{\ker\varphi} \simeq \operatorname{im}\varphi$, so $\mathbb{Q}[X]/_{I} \simeq \mathbb{Q}$.

2. $(X-2)$ and $(X+2)$ are not multiples of X^2-4 but their product is, therefore $\mathbb{Q}[X]/_{J}$ contains two nonzero elements α, β s.t $\alpha\beta = 0$ [illegible], so it's not a field.

1



Problem 2. (35 points)

1. Suppose $r\in\mathbb{Q}$ is a root of a polynomial
$$a_mX^m+a_{m-1}X^{m-1}+\ldots+a_0,\ \text{with } a_i\in\mathbb{Z},$$
and let $r=\frac{c}{d}$, with $c,d\in\mathbb{Z}$, and $\mathrm{GCD}(c,d)=1$. Then show that $c|a_0$ and $d|a_m$.
2. Show that X^3-3X-1 has no root in $\mathbb{Q}$ (hence it is irreducible in $\mathbb{Q}[X]$).(Hint: use the question just above...)
3. Let's call I the principal ideal generated by $P(X)=X^3-3X-1$. We write
$$\begin{array}{rccc}\varphi\colon & \mathbb{Q}[X] & \longrightarrow & \mathbb{Q}[X]/I\\ & T(X) & \longmapsto & T(X)\bmod I\end{array}$$
If we call $x=\varphi(X)$, then show that $1,x,x^2$ is a basis of the vector space $\mathbb{Q}[X]/I$.

1. If $a_m\left(\frac{c}{d}\right)^m+\cdots+a_0=0$, then by multiplying by d^m we get:

$$\underbrace{a_mc^m+a_{m-1}c^{m-1}.d+\cdots+}_{\text{multiple of } c}\ a_0d^m=0$$

, so $c|a_0d^m$ but G.C.D$(c,d)=1$, so $c|a_0$.

Similarly, one has $a_mc^m+\underbrace{a_{m-1}c^{m-1}.d+\cdots+a_0d^m}_{\text{multiple of } d}=0$, so necessarily $d|a_mc^m$, but G.CD$(c,d)=1$ so $d|a_m$.

2. Assume it has a root $\frac{c}{d}$, with G.C.D$(c,d)=1$, then by 1) we know that $d|1$ (so $d=\pm1$) and $c|-1$ (so $c=\pm1$)

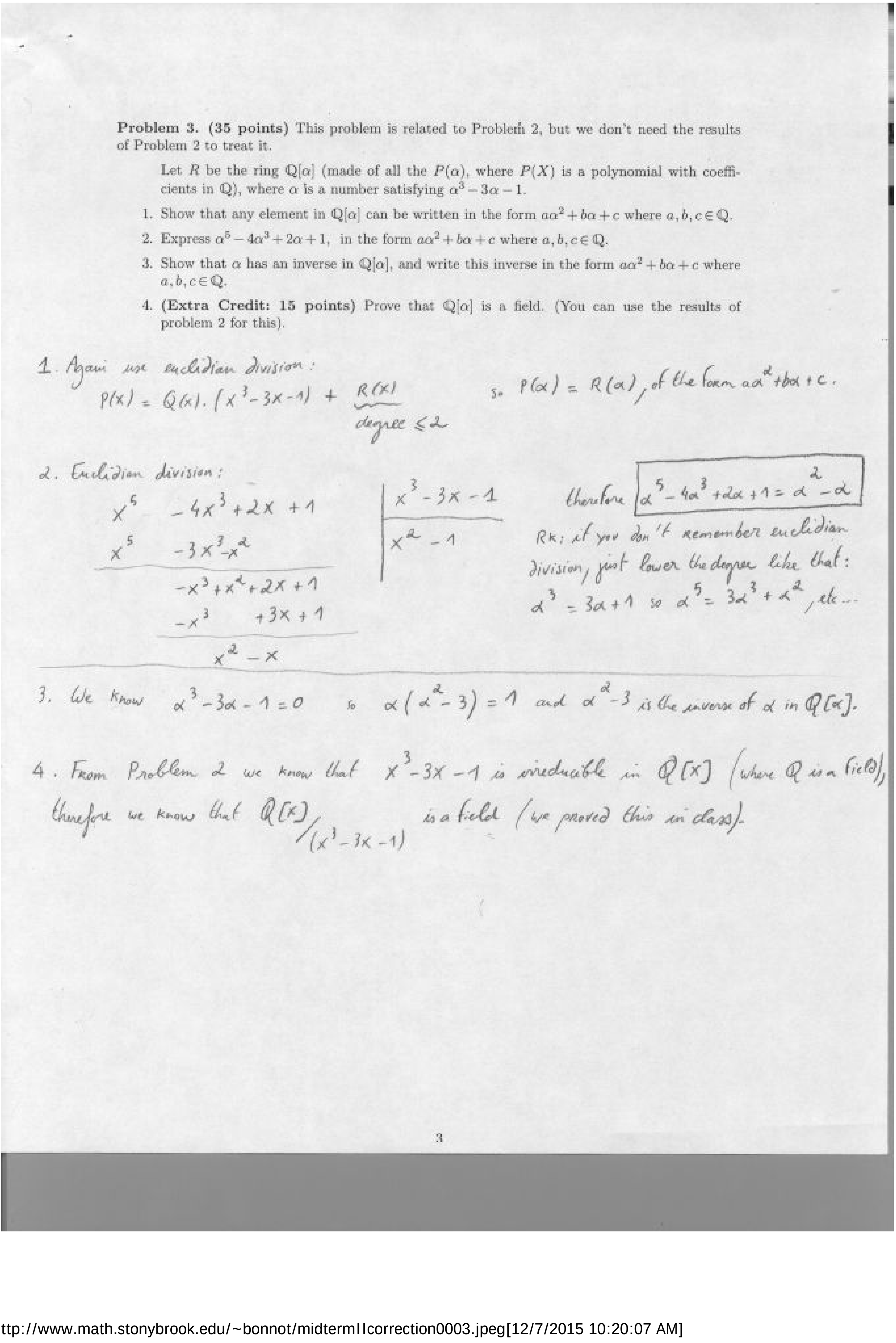
Thus the only possible roots in $\mathbb{Q}$ are ±1. But $\left.\begin{array}{l}P(1)=-3\neq0\\ P(-1)=+1\neq0\end{array}\right\}$

Therefore X^3-3X-1 has no root in $\mathbb{Q}$.

3. Write the euclidian division by X^3-3X-1: any polynomial $Q(X)=S(X).(X^3-3X-1)+\underbrace{R(X)}_{\text{of degree}\leq2}$

Since $Q(X)\bmod I=R(X)\bmod I$, any element in $\mathbb{Q}[X]/_I$ is a linear combination of $1,x,x^2$

Now assume $1,x,x^2$ are not linearly independent: there would exist a polynomial $a+bx+cx^2$ that would be 0 in $\mathbb{Q}[X]/_I$, thus the polynomial $a+bX+cX^2$ would be a multiple of X^3-3X-1 (impossible, because of the degree). Therefore $1,x,x^2$ is a basis.



Problem 3. (35 points) This problem is related to Problem 2, but we don't need the results of Problem 2 to treat it.

Let R be the ring $\mathbb{Q}[\alpha]$ (made of all the $P(\alpha)$, where $P(X)$ is a polynomial with coefficients in $\mathbb{Q}$), where α is a number satisfying $\alpha^3-3\alpha-1$.

1. Show that any element in $\mathbb{Q}[\alpha]$ can be written in the form $a\alpha^2+b\alpha+c$ where $a,b,c\in\mathbb{Q}$.
2. Express $\alpha^5-4\alpha^3+2\alpha+1$, in the form $a\alpha^2+b\alpha+c$ where $a,b,c\in\mathbb{Q}$.
3. Show that α has an inverse in $\mathbb{Q}[\alpha]$, and write this inverse in the form $a\alpha^2+b\alpha+c$ where $a,b,c\in\mathbb{Q}$.
4. **(Extra Credit: 15 points)** Prove that $\mathbb{Q}[\alpha]$ is a field. (You can use the results of problem 2 for this).

1. Again use euclidian division:

$$P(X) = Q(X).(X^3-3X-1) + \underbrace{R(X)}_{\text{degree} \leq 2} \qquad \text{so } P(\alpha) = R(\alpha), \text{ of the form } a\alpha^2+b\alpha+c.$$

2. Euclidian division:

$$\begin{array}{r|l} X^5 \quad -4X^3+2X+1 & X^3-3X-1 \\ \hline X^5 \quad -3X^3-X^2 & X^2-1 \\ \hline -X^3+X^2+2X+1 & \\ -X^3 \quad\quad +3X+1 & \\ \hline X^2-X & \end{array}$$

therefore $\boxed{\alpha^5-4\alpha^3+2\alpha+1=\alpha^2-\alpha}$

Rk: if you don't remember euclidian division, just lower the degree like that: $\alpha^3=3\alpha+1$ so $\alpha^5=3\alpha^3+\alpha^2$, etc...

3. We know $\alpha^3-3\alpha-1=0$ so $\alpha(\alpha^2-3)=1$ and α^2-3 is the inverse of α in $\mathbb{Q}[\alpha]$.

4. From Problem 2 we know that X^3-3X-1 is irreducible in $\mathbb{Q}[X]$ (where $\mathbb{Q}$ is a field), therefore we know that $\mathbb{Q}[X]/(X^3-3X-1)$ is a field (we proved this in class).

Problem 1. *Let $\epsilon = 1+\sqrt{2}$. Write $\epsilon^n = u_n + v_n\sqrt{2}$. Show that $u_n^2 - 2v_n^2 = \pm 1$.*

Answer. As in the first midterm, by hand,you can prove that $N(a+b\sqrt{2}) = a^2 - 2b^2$ is a multiplicative function. Therefore $N(\epsilon^n) = (N(\epsilon))^n = (1-2)^n = \pm 1$.

Problem 2. Structure of the invertible elements in $\mathbb{Z}[\sqrt{2}]$.

1. *Show that there is no invertible element $\alpha \in \mathbb{Z}[\sqrt{2}]$ such that $1 < \alpha < 1+\sqrt{2}$.*

2. *Deduce that any invertible element (greater than 0) of $\mathbb{Z}[\sqrt{2}]$ is a power of $1+\sqrt{2}$.*

Answer.

1. If there is such an $\alpha = a + b\sqrt{2}$ then $a - b\sqrt{2} = \pm\alpha^{-1}$ (because $(a + b\sqrt{2}).(a-b\sqrt{2}) = \pm 1$) and therefore $-1 < a - b\sqrt{2} < 1$. If you add the two inequalities together, you find $0 < 2a < 2+\sqrt{2} < 3.5$, and thus one must have $a = 1$. But now there doesn't exist any integer b such that $1 < 1 + b\sqrt{2} < 1+\sqrt{2}$.

2. It is enough to prove the result for invertible elements larger than 1. Such an invertible element β will land between two consecutive powers $(! + \sqrt{2})^n \leq \beta < (1+\sqrt{2})^{n+1}$ and therefore $1 \leq \frac{\beta}{(1+\sqrt{2})^n} < 1+\sqrt{2}$. Since the strict inequality is impossible, one must have $\beta = (1+\sqrt{2})^n$.

Problem 3. *Let R be the ring $\mathbb{Q}[\alpha]$ (meaning all the $P(\alpha)$, where P is a polynomial with coefficients in $\mathbb{Q}$), where α is a number satisfying $\alpha^3 - \alpha^2 + \alpha + 2 = 0$.*

1. *express $(\alpha^2 + \alpha + 1).(\alpha^2 - \alpha)$ in the form $a\alpha^2 + b\alpha + c$, where a, b, c are in $\mathbb{Q}$.*

2. *express $(\alpha - 1)^{-1}$ in the form $a\alpha^2 + b\alpha + c$, where a, b, c are in $\mathbb{Q}$.*

Answer.

1. expand the polynomial. Whenever you see a high power of α, replace it with a smaller one using the identity $\alpha^3 = \alpha^2 - \alpha - 2$.

2. The equality $\alpha^3 - \alpha^2 + \alpha + 2 = 0$ can be rewritten as $\alpha^2.(\alpha - 1) + \alpha - 1 + 3 = 0$ which gives $(\alpha - 1)(\alpha^2 + 1) = -3$, so the inverse will be $-\frac{1}{3}\alpha^2 - \frac{1}{3}$.

Problem 4. *Let $f : A \to B$ be a ring morphism. Show that for any prime ideal $\mathcal{P}$ in B, then $f^{-1}(\mathcal{P})$ is a prime ideal of A.*

Answer. Showing that $f^{-1}(\mathcal{P})$ is an ideal has been done in class. Let's prove it is a prime ideal: if $x.y \in f^{-1}(\mathcal{P})$ then $f(x).f(y) \in \mathcal{P}$. Since $\mathcal{P}$ is prime then necessarily $f(x) \in \mathcal{P}$ or $f(y) \in \mathcal{P}$, implying that x or y is in $f^{-1}(\mathcal{P})$.

Math 311 — Practice Midterm II

The actual midterm II will be shorter than the first one (it doesn't mean easier...)! There might be 3 problems.

Problem 1. *Let $\epsilon = 1 + \sqrt{2}$. Write $\epsilon^n = u_n + v_n\sqrt{2}$. Show that $u_n^2 - 2v_n^2 = \pm 1$.*

Problem 2. Structure of the invertible elements in $\mathbb{Z}[\sqrt{2}]$.

1. *Show that there is no invertible element $\alpha \in \mathbb{Z}[\sqrt{2}]$ such that $1 < \alpha < 1 + \sqrt{2}$.*
2. *Deduce that any invertible element (greater than 0) of $\mathbb{Z}[\sqrt{2}]$ is a power of $1 + \sqrt{2}$.*

Problem 3. *Let R be the ring $\mathbb{Q}[\alpha]$ (meaning all the $P(\alpha)$, where P is a polynomial with coefficients in $\mathbb{Q}$), where α is a number satisfying $\alpha^3 - \alpha^2 + \alpha + 2 = 0$.*

1. *express $(\alpha^2 + \alpha + 1).(\alpha^2 - \alpha)$ in the form $a\alpha^2 + b\alpha + c$, where a, b, c are in $\mathbb{Q}$.*
2. *express $(\alpha - 1)^{-1}$ in the form $a\alpha^2 + b\alpha + c$, where a, b, c are in $\mathbb{Q}$.*

Problem 4. *Let $f : A \to B$ be a ring morphism. Show that for any prime ideal $\mathcal{P}$ in B, then $f^{-1}(\mathcal{P})$ is a prime ideal of A.*

MAT 311 03/06/2007

Correction of Midterm i

Problem 1. (20 points) Assume that a, m are two integers such that $G.C.D(a,m)=1$.

1. Why does there exist an integer x_1 such that $a.x \equiv 1 (\operatorname{mod} m)$?
2. For $s = 1, 2, \ldots$ let $x_s = \frac{1}{a} - \frac{1}{a}(1 - a.x_1)^s$. Prove that x_s is an integer and that it is a solution of $a.x \equiv 1 (\operatorname{mod} m^s)$.

Proof.

1. Since $G.C.D.(a,m)=1$ there exist integers x, y such that $a.x + m.y = 1$, therefore $a.x \equiv 1$.
2. Expand $(1 - a.x_1)^s = 1 + \sum_{k=1}^{s} \binom{s}{k}.(-a.x_1)^k$, but all the $(a.x_1)^k$, $k \geqslant 1$ are multiples of a, therefore $\frac{1}{a}.\sum_{k=1}^{s} \binom{s}{k}.(-a.x_1)^k$ is an integer x_s.

Problem 2. (30 points) Let R be the ring $\left\{ a + b\sqrt{3} \middle/ a, b \in \mathbb{Z} \right\}$. We define a function N by:

$$\begin{array}{rccc} N\colon & R & \longrightarrow & \mathbb{Z} \\ & a + b\sqrt{3} & \longmapsto & a^2 - 3b^2 \end{array}$$

(Notice that N is not the square of the distance from 0 to α).

1. Show that $N(\alpha.\beta) = N(\alpha).N(\beta)$ for every α, β in R.
2. If α has an inverse in R for the multiplication, show that $N(\alpha) = 1$.(**Hint**: first show that $N(\alpha)$ must be ± 1, and then show that it can't be -1).
3. Conversely, show that if $N(\alpha) = 1$ then α has an inverse in R.
4. Find 4 distinct examples of invertible elements in R.

Proof.

1. If $\alpha = a + b\sqrt{3}$, $\beta = c + d\sqrt{3}$ then $\alpha.\beta = (\mathrm{ac} + 3\mathrm{bd}) + (\mathrm{ad} + \mathrm{bc})\sqrt{3}$, so $N(\alpha.\beta) = (\mathrm{ac} + 3\mathrm{bd})^2 - 3(\mathrm{ad} + \mathrm{bc})^2 = a^2c^2 + 6\mathrm{abcd} + 9b^2d^2 - 3a^2d^2 - 6\mathrm{abcd} - 3b^2c^2$,
   whereas $N(\alpha).N(\beta) = (a^2 - 3b^2).(c^2 - 3d^2) = a^2c^2 - 3a^2d^2 + 9b^2d^2 - 3b^2c^2$, the same.
2. $(\alpha.\beta = 1) \Rightarrow N(\alpha).N(\beta) = 1$, where $N(\alpha), N(\beta) \in \mathbb{Z}$, so necessarily $N(\alpha) = \pm 1$.
   Now $a^2 - 3b^2 = -1$ is impossible because $a^2 + 1$ (mod 3) takes only the values 1 or 2.
3. $N(\alpha) = 1 \Rightarrow a - \sqrt{3}b \in R$ is the inverse of α, because $(a + b\sqrt{3}).(a - b\sqrt{3}) = a^2 - 3b^2 = 1$
4. 1,-1,$2 + \sqrt{3}$,$2 - \sqrt{3}$ are examples, but then are lots of other examples.

Problem 3. (20 points) You probably remember that in class we proved that the (multiplicative) group of invertible elements of $\mathbb{Z}/p\mathbb{Z}$ is cyclic (for p prime).

1. Show that $(\mathbb{Z}/8\mathbb{Z})^\times$ (this means the multiplicative group of invertible elements in $\mathbb{Z}/8\mathbb{Z}$) is not cyclic. (Hint: what are the orders of the elements of $(\mathbb{Z}/8\mathbb{Z})^\times$?)
2. (**Extra credit: 15 points**) Can you deduce from above that the same result is true for higher powers (I mean in $\mathbb{Z}/2^n\mathbb{Z}$, for $n \geqslant 3$)? (try 2^4 or 2^5, because a general proof is harder to obtain).

Proof.

Just realize that $(\mathbb{Z}/8\mathbb{Z})^\times = \{1, 3, 5, 7\}$ and that all these elements are of order 2 (their squares are $\equiv 1 (\operatorname{mod} 8)$).

You can do the same for $\mathbb{Z}/16\mathbb{Z}$. In class I might indicate a general proof.

Problem 4. (30 points) We call $\sigma(n)$ the sum of all the divisors of the integer n. For example $\sigma(6) = 1 + 2 + 3 + 6 = 12$, and $\sigma(5) = 1 + 5 = 6$.

1. For any prime p, any integer $k \geqslant 1$, show that $\sigma(p^k) = \frac{p^{k+1} - 1}{p - 1}$.
2. If $G.C.D(m, n) = 1$ prove that $\sigma(m.n) = \sigma(m).\sigma(n)$. If you can't prove this then prove the simpler case $\sigma(p.q) = \sigma(p).\sigma(q)$, when p, q are two distinct primes.
3. Give a general formula for $\sigma(n)$ in terms of its decomposition in prime factors $n = p_1^{k_1} ... p_n^{k_n}$

Proof.

1. The only divisors of p^k are $1, p, p^2, ..., p^k$. Their sum is $\sum_{i=1}^{k} p^i = \frac{p^{k+1} - 1}{p - 1}$.
2. Let's write $m = p_1^{r_1} ... p_k^{r_k}$, and $n = q_1^{s_1} ... q_l^{s_l}$ where the p_i and the q_j are distinct. Then each divisor of $m.n$ can be written in a unique way as $\left(\prod p_i^{t_i} \right) . \left(\prod q_j^{t_j} \right)$, therefore these divisors of $m.n$ are in bijection with the ordered pairs (a, b) where a is a divisor of m, and b a divisor of n.Since $\sigma(m).\sigma(n)$ is the sum of all products (divisor of m).(divisor of n), we get the result.
3. From above, one derives $\sigma(n) = \prod_{i=1}^{n} \frac{p_i^{k_i+1} - 1}{p_i - 1}$.

Remark.

One could solve the whole problem in one step, by expanding the product

$$S = (1 + p_1 + ... + p^k)...(1 + p_n + ... + p_n^{k_n})$$

and noticing that one gets exactly the sum of all divisors of n

Math 311 — Practice Midterm I

Since you will have only one hour for the exam, the actual exam should be shorter than that...I include more problems so that you can practice!

Problem 1. *Solve the congruence* $x^3 + 4x + 8 \equiv 0$ *(mod 15)* .

Answer. Using the Chinese remainder theorem, we see that this congruence has a solution if and only if it has one solution modulo 3 and one solution modulo 5. Now by hand one can realize that the congruence modulo 5 has no solution, so the problem has no solution.

Problem 2. *Show that* $\phi(nm) = n\phi(m)$ *if every prime that divides n also divides m.*

Answer. Just write $n = p_1^{r_1} \ldots p_k^{r_k}$ and $m = p_1^{s_1} \ldots p_k^{s_k}.m'$ where m' is coprime with n. Now one has

$$\phi(n.m) = \phi(p_1^{r_1+s_1} \ldots p_k^{r_k+s_k}.m') = (p_1^{r_1+s_1} - p_1^{r_1+s_1-1}) \ldots (p_k^{r_k+s_k} - p_k^{r_k+s_k-1}).\phi(m'),$$

but this is also $(p_1^{r_1} \ldots p_k^{r_k}).(p_1^{s_1} - p_1^{s_1-1}) \ldots (p_k^{s_k} - p_k^{s_k-1}).\phi(m') = n.\phi(m)$.

Problem 3. *How many square roots of* 1 *are there in* $\mathbb{Z}/3\mathbb{Z}$*? in* $\mathbb{Z}/5\mathbb{Z}$*? in* $\mathbb{Z}/15\mathbb{Z}$*? in* $\mathbb{Z}/p.q\mathbb{Z}$ *(where p,q are two distinct primes)?*

Answer. Since $\mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/5\mathbb{Z}$ are fields, the equation $X^2 - 1 = 0$ has exactly two roots ± 1. Now because of the chinese remainder theorem, we know the existence of the isomorphism

$$\mathbb{Z}/15\mathbb{Z} \longrightarrow \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}.$$

Since this map is a ring morphism there is a bijection between the roots of $X^2 - 1 \bmod 15$ and the ordered pairs $(a, b) \in \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, where $a^2 - 1 \equiv 0 \bmod 3$, and $b^2 - 1 \equiv 0 \bmod 5$. So we get 4 such roots. The same thing is true for $\mathbb{Z}/p.q\mathbb{Z}$

Problem 4. *Let p be an odd prime.Assume that* $x \in \mathbb{Z}/p\mathbb{Z}$ *is a generator of the (cyclic) multiplicative group of* $(\mathbb{Z}/p\mathbb{Z})$*. Does x have a square root in* $\mathbb{Z}/p\mathbb{Z}$*?*

Answer. If there is such a square root y of x, then one could write it as $y = x^k$ for some $1 \leq k \leq p - 1$ because x is a generator. But then one has $x = y^2 = x^{2k}$, so $x^{2k-1} - 1 \equiv 0$. Since the order of x is $p - 1$ this implies $p - 1 | 2k - 1$, but since $2k - 1 < 2p - 1 < 2(p - 1)$, the only possibility is $2k - 1 = p - 1$ (absurd: p must be odd).

Problem 5. *Show that if p is an odd prime and* $G.C.D.(a, p) = 1$ *then* $x^2 \equiv a(\text{ mod } p^\alpha)$ *(where* α *is an integer* ≥ 1*) has exactly* $1 + (\frac{a}{p})$ *solutions, where* $(\frac{a}{p})$ *is equal to* $+1$ *if the integer a has a square root modulo p, and is equal to* -1 *otherwise.*

Answer.

- If $(\frac{a}{p}) = -1$, then clearly $x^2 = a \bmod p^\alpha$ has no root (otherwise it would have a root modulo p);

- now assume $(\frac{a}{p}) = +1$: if the equation $x^2 = a \bmod p^\alpha$ has one solution b, then automatically it has also the solution $-b$ (just because $(-1)^2 = 1$!). Let's show that it can't have a third root c with $c \neq b$ and $c \neq -b$. Indeed one would have $b^2 = a = c^2$, and therefore $p^\alpha | (b-c).(b+c)$. But since modulo p^α one has $c \neq b$ and $c \neq -b$, this would imply that p divides both $b-c, b+c$ and therefore p would divide b and also a (impossible because a and p are coprime). At this point we have proved that if there is one solution, then there are actually exactly two solutions. So it remains to prove the existence of one solution modulo p^α, knowing that there is a solution modulo p. Here the integer a is fixed, and we can assume that it is less than p^α. By successive euclidian divisions by the power of p, one can write it as $a = a_0 + pa_1 + \ldots + p^{\alpha-1}.a_{\alpha-1}$. (Replace p by 10 and this is just the usual form of an integer in base 10...).There is a solution modulo p, so there is an x, $x \leq p$ such that $x^2 \equiv a \bmod p$. As an integer one has $x^2 = c + p.d$. Necessarily $c = a_0$. Now replace x by $x + b.p$, where $b < p$: then $(x + p.b)^2 = x^2 + 2b.x.p + b^2.p^2$. Since $2.b.x$ can take all the possible values modulo p, one can find a b such that $x^2 \equiv a$ modulo p^2. Let's prove by induction that one can find a solution modulo p^α: Assume one has a solution x modulo p^k, with $x < p^k$. Then $x^2 = a_0 + \ldots + a_{k-1}p^{k-1} + C.p^k$, where C can be expanded in powers of p as a finite sum $C_0 + pC_1 + \ldots$. The only thing we have to do is to replace x by $x' = x + t.p^\alpha$, so that now $x'^2 = a_0 + \ldots + a_{k-1}p^{k-1} + a_k.p^k + C'.p^{k+1}$. But again, just write $x' = x + t.p^k$, notice that since $2x$ is prime with p, the multiples $2t.x$ can take any value modulo p, and therefore $x^2 + 2t.x.p^k + t^2.p^{2k}$ can be made congruent to a modulo p^{k+1}. Thus we proved that if there is one square root modulo p then there are exactly two $(2 = 1 + (\frac{a}{p}))$ square roots modulo p^α.

Problem 6. *We write $j = e^{\frac{2i\pi}{3}}$ and consider the set $R = \{a + bj | a, b \in \mathbb{Z}\}$.*

- *Show that R is a subring of $\mathbb{C}$;*
- *What are the invertible elements of R? (Hint: show that the square of the modulus of such an element z, which is $|z|^2 = z.\bar{z}$, must be 1).*

Answer. The only thing to realize is that the product $j.j = j^2 = -1 - j$ is in the ring. Now the square of the modulus of $a + b.j$ is $a^2 + b^2 - ab$ and it must be a positive invertible integer, so it must be 1. Now $a \geq 2, b \geq 2$ are impossible, so a, b must be in $\{-1, 0-1\}$. This leaves only six possibilities : $\{1, -1, j, j^2, 1 + j, -1 - j\}$.

Problem 7. bonus problem *Can you prove that R in the previous problem is a "principal ideal domain" (meaning that any ideal I can be written as the set of all multiples of one single element)? You can use results of the HWs...*

Answer. You just need to prove that around the origin there is a disk containing only the origin as a point of R, and that there exists for any complex number z in the plane an element λ of R such that $|z - \lambda| < 1$.

1 Review Midterm 1

Here are some informations about what you should know for the test...Feel free to ask me any questions about that during the week (even outside the regular office hours)!

1 Basic arithmetic

- Notion of divisibility, prime numbers, G.C.D.
- Euclidian division in $\mathbb{Z}$, the Euclidian algorithm (for the determination of a G.C.D.)
- Proof of: ''The additive subgroups of $\mathbb{Z}$ are the $n\mathbb{Z}$''
- Definition of G.C.D(m,n) as the positive integer d such that $d\mathbb{Z} = m\mathbb{Z} + n\mathbb{Z}$.
- Proof of : ''$\sqrt{2} \notin \mathbb{Q}$.
- Definition of $\phi(n)$, $\phi(m.n) = \phi(m).\phi(n)$ if $G.C.D.(m, n) = 1$.

2 Congruences

- The ideals of the ring $\mathbb{Z}$ are the $n\mathbb{Z}$
- definition of the ring $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ and how to compute with congruences.
- $(\mathbb{Z}/n\mathbb{Z}, +)$ is an additive cyclic group.
- $(\mathbb{Z}/p\mathbb{Z}, , +, \times)$ is a field if and only if p is prime (you need to know how to prove this).
- The multiplicative group $(\mathbb{Z}/p\mathbb{Z}^{\times}, \times)$ is cyclic of order $p-1$, when p is prime.
- Little Fermat's theorem.

3 Rings and ideals

- Definition of a ring, of a ring morphism, kernel and image of a ring morphism
- Definitions: of an ideal, sum of two ideals $(I + J)$, intersection, product of two ideals
- Quotient of a ring by an ideal

Theorem 1. *(Chinese Remainder Theorem) Let I, J be two ideals of the ring R, such that $I + J = R$, then there is an isomorphism*

$$R/(I.J) \simeq R/I \times R/J$$

given by

$$r \bmod I.J \longmapsto (r \bmod I, r \bmod J)$$

- Definition of the characteristic of a field
- In a field of characteristic p, one has $(x + y)^p = x^p + y^p$.

- If $f\colon R\to S$ is a ring morphism, then $f\colon R\to \mathrm{im}\ f$ is surjective, and $\bar{f}: R/\ker f\to \mathrm{im}\ f$ defined by $r \bmod \ker f\longmapsto f(r)$ is well defined and is an isomorphism.
- $\mathbb{R}[X]/(X^2+1)\simeq\mathbb{C}$ as an example of the theorem just above.

4 Quadratic reciprocity

Definition 2. *The* ***Legendre symbol*** $\left(\frac{a}{p}\right)$*, where* p *is an odd prime, and* a *is any integer is equal to* $+1$ *if* a *has a square root in* $\mathbb{Z}/p\mathbb{Z}$*, and* -1 *otherwise.*

I would like you to know the following result and to have a vague idea of the proof

Theorem 3. *(Legendre, Gauss) If* p *and* q *are two odd primes, then*

$$\left(\frac{p}{q}\right).\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}.\frac{q-1}{2}}.$$

- $\left(\frac{a}{p}\right)=a^{\frac{p-1}{2}} \bmod p$ and how to prove it.

5 Basic cryptography

- just know the R.S.A system (as it is explained at the beginning of the HW5).
- understand why there are 4 square roots of 1 in $\mathbb{Z}/p.q\mathbb{Z}$, when p, q are two distinct primes (answer: chinese remainder theorem).

Math 311 Practice Midterm I

Since you will have only one hour for the exam, the actual exam should be shorter than that...I include more problems so that you can practice!

Problem 1. *Solve the congruence* $x^3 + 4x + 8 \equiv 0$ *(mod 15) .*

Problem 2. *Show that* $\phi(nm) = n\phi(m)$ *if every prime that divides n also divides m.*

Problem 3. *How many square roots of* 1 *are there in* $\mathbb{Z}/3\mathbb{Z}$*? in* $\mathbb{Z}/5\mathbb{Z}$*? in* $\mathbb{Z}/15\mathbb{Z}$*? in* $\mathbb{Z}/p.q\mathbb{Z}$ *(where p,q are two distinct primes)?*

Problem 4. *Let p be an odd prime.Assume that* $x \in \mathbb{Z}/p\mathbb{Z}$ *is a generator of the (cyclic) multiplicative group of* $(\mathbb{Z}/p\mathbb{Z})$*. Does x have a square root in* $\mathbb{Z}/p\mathbb{Z}$*?*

Problem 5. *Show that if p is an odd prime and* $G.C.D.(a,p) = 1$ *then* $x^2 \equiv a(\text{ mod } p^\alpha)$ *(where* α *is an integer* ≥ 1*) has exactly* $1 + (\frac{a}{p})$ *solutions, where the symbol* $(\frac{a}{p})$ *is equal to* $+1$ *if a has a square root modulo p, and* -1 *otherwise.*

Problem 6. *We write* $j = e^{\frac{2i\pi}{3}}$ *and consider the set* $R = \{a + bj | a, b \in \mathbb{Z}\}$.

- *Show that R is a subring of* $\mathbb{C}$*;*
- *What are the invertible elements of R? (Hint: show that the square of the modulus of such an element z, which is* $|z|^2 = z.\bar{z}$*, must be* 1*).*

Problem 7. bonus problem *Can you prove that R in the previous problem is a "principal ideal domain" (meaning that any ideal I can be written as the set of all multiples of one single element)? You can use results of the HWs...*

1 Quadratic reciprocity

1 Proof (inspired by Serre)

Definition 1. *The* ***Legendre symbol*** $\left(\frac{a}{p}\right)$*, where* p *is an odd prime, and* a *is any integer is equal to* $+1$ *if* a *has a square root in* $\mathbb{Z}/p\mathbb{Z}$*, and* -1 *otherwise.*

Our goal is

Theorem 2. *(Legendre, Gauss) If* p *and* q *are two odd primes, then*

$$\left(\frac{p}{q}\right).\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}.\frac{q-1}{2}}.$$

Proof. Write $\zeta=e^{\frac{2\pi i}{p}}\in\mathbb{C}$. We will work in the subring $\mathbb{Z}[\zeta]\subseteq\mathbb{C}$. This is just the ring made of all polynomials in ζ.

Let's consider the so-called ''Gauss sum''

$$\tau=\sum_{a\in(\mathbb{Z}/p\mathbb{Z})^\times}\left(\frac{a}{p}\right)\zeta^a$$

It has many nice properties:

- First property: $\left(\frac{-1}{p}\right).\tau^2=p$

  Indeed, one has $\left(\frac{-1}{p}\right).\tau^2=\left(\frac{-1}{p}\right).\sum_{a,b}\left(\frac{a.b}{p}\right)\zeta^{a+b}=\sum_{a,b}\left(\frac{a.(-b)}{p}\right)\zeta^{a+b}$, because $\left(\frac{c}{p}\right).\left(\frac{d}{p}\right)=\left(\frac{c.d}{p}\right)$. One also has that $\left(\frac{c}{p}\right)=\left(\frac{c^{-1}}{p}\right)$ (because c has a square root if and only if its inverse has one.

  Thus $\sum_{a,b}\left(\frac{a.(-b)}{p}\right)\zeta^{a+b}=\sum_{a,b}\left(\frac{a.b}{p}\right)\zeta^{a-b}=\sum_{a,b}\left(\frac{a.b^{-1}}{p}\right)\zeta^{a-b}=\sum_{c,b}\left(\frac{c}{p}\right)\zeta^{b.c-b}$, just thanks to the change of variables $c=a.b^{-1}$.

  At this point, one can break the last sum in two groups $(c=1)$ and $(c\neq1)$ and get

  $$\left(\frac{-1}{p}\right).\tau^2=\left(\frac{1}{p}\right).\sum_b 1+\left(\sum_{c\neq1}\left(\frac{c}{p}\right)\right).\sum_{b\neq0}(\zeta^{c-1})^b=(p-1)+(-1).(-1)=p.$$

  Indeed: $\left(\frac{1}{p}\right)=1$, always, and $\sum_c\left(\frac{c}{p}\right)=0$, because there are as many elements that have a square root as elements that do not have a square root (multiply the first set by one element in the second set to get everybody in the second set!), and so $1+\sum_{c\neq1}\left(\frac{c}{p}\right)=0$. Now the last part is well-known to you: the sum of the $n-\mathrm{th}$ roots of unity is always zero.

- Second property: $\tau^q=\tau.(\tau^2)^{\frac{p-1}{2}}=\tau.(-1)^{\frac{p-1}{2}.\frac{q-1}{2}}.p^{\frac{q-1}{2}}$ mod p.

  Just use the first property and remember that $\left(\frac{a}{p}\right)=(-1)^{\frac{p-1}{2}}$ (We saw that earlier).

- Third property: $\tau^q=\left(\frac{q}{p}\right).\tau$ mod q

  Indeed if you remember that in $\mathbb{Z}/q\mathbb{Z}$ one has $(x+y)^q\equiv x^q+y^q$, then

  $$\tau^q=\sum_a\left(\frac{a}{p}\right)^q.\zeta^{a.q}=\sum_a\left(\frac{a}{p}\right).\zeta^{a.q}=\sum_a\left(\frac{a.q^2}{p}\right).\zeta^{a.q}=\left(\frac{q}{p}\right).\sum_a\left(\frac{a.q}{p}\right).\zeta^{a.q}=\left(\frac{q}{p}\right).\tau$$

Basically, $\left(\frac{q^2}{p}\right) = 1$, and since q is odd, $\left(\frac{a}{p}\right)^q = (\pm 1)^q = \pm 1$ which explains the line above.

Now we are done! Just put together property 2 and 3 (and remember that $p^{\frac{q-1}{2}} = \left(\frac{p}{q}\right)$).

□

Math 311 Homework 4 due on Fr. 02/23

Problem 1. *Let R be a subring of the complex numbers $\mathbb{C}$ having the following two properties:*

1. *There is a disk D around the origin $0 \in \mathbb{C}$, such that $D \cap R = \{0\}$;*
2. *For any $z \in \mathbb{C}$ there exists an element $\lambda \in R$ such that $|z - \lambda| < 1$.*

   Show that any ideal I of R is the set of the multiples of an element $a \in R$.

   Hint*: Show that, in any ideal I of R, there exists one element $b \in I$ that is different from 0, and that is at minimal distance from the origin. Show that the ideal I coincides actually with the set of multiples of b (namely show that $I = b.R$).*

Problem 2. *Let p be an odd prime and let $d = b^2 - 4ac$. Show that the congruence*

$$ax^2 + bx + c \equiv 0 \; (mod\ p)$$

is equivalent to the congruence $y^2 \equiv d \; (mod\ p)$, where $y = 2ax + b$. Conclude that if $d \equiv 0 \; (mod\ p)$, then there is exactly one solution modulo p; if d has a square root in $\mathbb{Z}/p\mathbb{Z}$, then there are two (non congruent) solutions; and if d has no square root in $\mathbb{Z}/p\mathbb{Z}$, then there are no solutions. What about the case $p = 2$?

Problem 3. *Consider $\mathbb{Z}[X]$, the set of polynomials with coefficients in $\mathbb{Z}$. Show that there are ideals in $\mathbb{Z}[X]$ that cannot be written as the set of multiples of a single polynomial.*

Hint*: consider the ideal generated by 2 and X (meaning: the ideal made of all the possible sums of one multiple of 2 and one multiple of X).*

Problem 4. *Go on the web and find a short description of the "ElGamal cryptosystem". Write a short (< 10 lines) description of this algorithm used for encryption.*

Problem 5. *Let p be an odd prime. Assume that in $\mathbb{Z}/p\mathbb{Z}$ there exists a nonzero element ζ such that*

- *ζ has no square root in $\mathbb{Z}/p\mathbb{Z}$;*
- *the order of ζ in the multiplicative group of $\mathbb{Z}/p\mathbb{Z}$ is exactly 4.*

  Show that 2 has no square root in $\mathbb{Z}/p\mathbb{Z}$.

Problem 1. *Find all the solutions in integers of* $71x - 50y = 1$.

Answer. First we notice that 71 and 50 are coprime (indeed 71 is prime, and 50 is not a multiple of it). Therefore we know that the problem has an infinity of solutions. Let's find one of it by Euclid's algorithm:

$$\begin{aligned} 71 &= 1.50 + 21 \\ 50 &= 2.21 + 8 \\ 21 &= 2.8 + 5 \\ 8 &= 1.5 + 3 \\ 5 &= 1.3 + 2 \\ 3 &= 1.2 + 1 \end{aligned}$$

And then we undo what we did:

$$\begin{array}{ccccc} 1 & = & 3-2 & = & 3-(5-3) \\ & & & = & 2.3-5 \\ & & & = & 2.(8-5)-5 \\ & & & = & 2.8-3.5 \\ & & & = & 2.8-3.(21-2.8) \\ & & & = & 8.8-3.21 \\ & & & = & 8.(50-2.21)-3.21 \\ & & & = & 8.50-19.21 \\ & & & = & 8.50-19.(71-50) \\ & & & = & 27.50-19.71 \end{array}$$

Therefore we know that the solutions are exactly of the form

$$\{(x,y)/x = -19 + 50t, y = -27 + 71t, t \in \mathbb{Z}\}.$$

Problem 2. *If a and b are any positive integers* > 2, *then prove that* $2^a + 1$ *is not divisible by* $2^b - 1$.

Answer. By Euclidian division, one can write $a = b.s + r$. So if we write $m = 2^b - 1$, one has

$$2^a + 1 \equiv 2^r.(2^b)^s + 1 \equiv 2^r + 1 (\text{mod } m)$$

Now notice that $b > 2$ implies that $m > 3$ therefore if $r = 0, 1$ then $0 \leq 2^r + 1 < m$ and m does not divide $2^r + 1$. Thus we can assume $r \geq 2$. Since we know $r + 1 \leq b$ we deduce $2.2^r \leq 2^b$ and so $2^r + 1 \leq 2^b - 2^r + 1 \leq 2^b - 2$ because $r \leq 2$ implies $1 - 2^r \leq -2$.

Problem 3. *Show that if* $G.C.D(a,b) = 1$ *then* $G.C.D.(a+b, a^2 - a.b + b^2) = 1$ *or* 3.

Answer. Let's call d the $G.C.D.(a+b, a^2-a.b+b^2)$. Then d must also divide $(a+b)^2$ and $a^2-a.b+b^2$, so it must divide their difference $3ab$. I claim that d and ab are relatively prime: indeed if p was a prime factor common to ab and d, then p should divide a or b, but also $a+b$, so it would divide both a and b (absurd). Therefore d must divide 3, which means that d is ± 1 or ± 3.

Problem 4. *Using congruences, show that 7 divides* $(3^{2n+1}+2^{n+2})$ *for all* $n \geqslant 1$.

Answer. It's simply a matter of seeing that

$$(3^{2n+1}+2^{n+2}) \equiv 3.2^n + 4.2^n \equiv 7.2^n \equiv 0(\text{ mod } 7)$$

because ($3^2 \equiv 2$).

Problem 5. *Find all the solutions of the congruence* $x^2+4x+2 \equiv 0(mod 7)$.

Answer. There are many different ways of solving this. One way is to compute the values taken by the polynomial X^2+4X+2 at the points $\{0,\dots,6\}$, and find out when this is 0 mod 7. Or you can notice that $x^2+4x+2 \equiv x^2-3x+2 \equiv (x-1)(x-2)$. But since $\mathbb{Z}/7\mathbb{Z}$ is a field $(x-1)(x-2) \equiv 0$ is equivalent to $x \equiv 1$ or $x \equiv 2$, which is the answer.

Problem 6. *Consider a polygon centered on the origin and that is regular with m sides (regular means that all the sides have same length). You can go in the counterclockwise direction and number all the vertices from 1 to m. Consider now a counterclockwise rotation (with center the origin) that brings the vertex 1 to the vertex $1+k$, where k and m are coprime. Can you show that by iterating this same rotation you will visit all the vertices of the polygon?*

Answer. By a rotation-dilation centered at the origin, one can bring the vertices of our regular polygon to the $m-$th roots of the unity $\{1, e^{i\frac{2\pi}{m}}, \dots, e^{i\frac{2\pi}{m}(m-1)}\}$. Therefore the rotation we consider corresponds to the multiplication by $e^{i\frac{2\pi}{m}(k)}$. Now we have seen that $G.C.D(k,m)=1$ implies that there exists integers s,t such that $1=s.k+t.m$. Therefore

$$e^{i\frac{2\pi}{m}} = (e^{i\frac{2\pi}{m}(k)})^s.(e^{i\frac{2\pi}{m}(m)})^t = (e^{i\frac{2\pi}{m}(k)})^s$$

But we are done now because we know that by multiplying by $\frac{2\pi}{m}$ we can get all the $m-$th roots of the unity.

Math 311 — Homework 3 due on Fr. 02/16

Problem 1. *Characterize the set of positive integers n such that* $\phi(2n) > \phi(n)$.

Problem 2. *What are the last two digits, that is the tens and units digits of* $2^{1000}, 3^{1000}$*?*

Problem 3. *Prove that for* $n \geq 2$ *the sum of all the positive integers less than n and coprime with n is* $\frac{n}{2}.\phi(n)$.

Problem 4. *Find all the primes p such that p divides* $2^p + 1$.

Problem 5. *Show that* $x^2 - 2y^2 + 8z = 3$ *has no solutions* $(x, y, z) \in \mathbb{Z}^3$. (**Hint:** *reduce modulo 8).*

Problem 6. *For any n show that* $\phi(n) = n.(1 - \frac{1}{p_1}) \ldots (1 - \frac{1}{p_k})$ *where the* p_i *are the prime factors present in the prime decomposition of n.* (**Hint:**: *compute first* $\phi(p^s)$*, for any prime p.)*

HW 2

Due on Friday 02/09

Exercise 1. Find all the solutions in integers of $71x - 50y = 1$.

Exercise 2. If a and b are any positive integers > 2, then prove that $2^a + 1$ is not divisible by $2^b - 1$.

Exercise 3. Show that if $G.C.D(a, b) = 1$ then $G.C.D.(a + b, a^2 - a.b + b^2) = 1 \text{ or } 3$.

Exercise 4. Using congruences, show that 7 divides $(3^{2n+1} + 2^{n+2})$ for all $n \geqslant 1$.

Exercise 5. Find all the solutions of the congruence $x^2 + 4x + 2 \equiv 0 (\text{mod } 7)$.

Exercise 6. Consider a polygon centered on the origin and that is regular with m sides (regular means that all the sides have same length). You can go in the counterclockwise direction and number all the vertices from 1 to m. Consider now a counterclockwise rotation (with center the origin) that brings the vertex 1 to the vertex $1 + k$, where k and m are coprime. Can you show that by iterating this same rotation you will visit all the vertices of the polygon?

HW 1

This is due Friday February 2nd.

1. Show that the map $f\colon \mathbb{N}^2 \to \mathbb{N}$ given by:

$$f(x,y) = x + \frac{(x+y).(x+y+1)}{2}$$

is surjective. (We already proved it was injective, therefore it will be bijective).

2. Is the number $\sqrt{2} + \sqrt{3}$ a rational number?

3. Prove by induction that

$$\sum_{i=1}^{n} k^3 = \left[\frac{n.(n+1)}{2}\right]^2.$$

4. Prove that $n^5 - n$ is divisible by 30, for any integer n.

5. We have seen examples of "twin primes" p, q (their difference is equal to ± 2). Let p and q be two primes: show that pq + 1 is the square of an integer if and only if p and q are twin primes.

6. Draw the hyperbola $\mathcal{H}$: $\left\{(x,\, y) \in \mathbb{R}^2 / x^2 - y^2 = 1\right\}$. Find all the points on $\mathcal{H}$ that have rational coordinates.

Hint: Take the half-lines starting from $(-1,\, 0)$ and having a rational slope and see where they intersect the hyperbola.

Problem 1. *Show that the map $f : \mathbb{N}^2 \to \mathbb{N}$ given by:*

$$f(x,y) = x + \frac{(x+y).(x+y+1)}{2}$$

is surjective. (We already proved it was injective, therefore it will be bijective).

Answer. The sequence $M \mapsto \frac{M.(M+1)}{2}$ is strictly increasing. Therefore for any natural number L, there exists a unique M such that:

$$\frac{M.(M+1)}{2} \leqslant L < \frac{(M+1).(M+2)}{2}.$$

Notice now that $0 \leqslant L - \frac{M.(M+1)}{2} < \frac{(M+1).(M+2)}{2} - \frac{M.(M+1)}{2} = M+1$.

Therefore we can set: $0 \leqslant x = L - \frac{M.(M+1)}{2}$ and $y = M - x$. The key fact is that the inequality above implies that $M - x \geqslant 0$. Now by construction we have

$$L = x + \frac{M.(M+1)}{2} = f(x,y).$$

Problem 2. *Is the number $\sqrt{2} + \sqrt{3}$ a rational number?*

Answer. If this number was rational then its square $5 + 2\sqrt{6}$ would be rational and therefore $\sqrt{6}$ would also be rational. So we would have $\sqrt{6} = \frac{p}{q}$ where we can assume that the fraction is simplified (meaning that $G.C.D(p,q) = 1$).

But then

$$6.q^2 = p^2$$

so 6 would divide p (thus $p = 6.t$), and therefore $6.q^2 = 36.t^2$ implying that $6|q$ (absurd because the fraction was simplified).

Problem 3. *Prove by induction that*

$$\sum_{k=1}^{n} k^3 = \frac{n^2.(n+1)^2}{4}$$

Answer.

1. True for $n = 1$ because $1 = 1$;
2. Assume that

$$\sum_{k=1}^{n} k^3 = \frac{n^2.(n+1)^2}{4},$$

Then we have:

$$\sum_{k=1}^{n+1} k^3 = \frac{n^2.(n+1)^2}{4} + (n+1)^3 = \frac{(n+1)^2}{4}.(n^2 + 4.(n+1)) = \frac{(n+1)^2}{4}.(n+2)^2$$

Problem 4. *Prove that $n^5 - n$ is divisible by 30, for any integer n.*

Answer. One has $N = n^5 - n = n.(n-1).(n+1).(n^2+1)$. Since $n-1, n, n+1$ are three consecutive numbers, one of them at least is even, and one of them is a multiple of 3.

Now, if $n = 5k, \text{or} 5k+1, \text{or} 5k-1$ then one of these consecutive numbers is a multiple of 5. The only other possibilities are $n = 5k \pm 2$, but then $n^2 + 1 = 25k^2 \pm 20k + 4 + 1$ which is a multiple of 5.

Thus we know that the prime factors $2, 3, 5$ are present in the decomposition of N, so N is a multiple of 30.

Problem 5. *We have seen examples of "twin primes" p, q (their difference is equal to ± 2). Let p and q be two primes: show that $pq + 1$ is the square of an integer if and only if p and q are twin primes.*

Answer. If p, q are twin primes, then, say, $q = p + 2$ and then $p.q + 1 = p^2 + 2p + 1 = (p+1)^2$.

In the other direction:

if $p.q = n^2 - 1 = (n-1).(n+1)$, since p, q are primes we know that $n^2 - 1 \geqslant p.q \geqslant 2.2 = 4$, so $n^2 \geqslant 5$ and this implies that n is at least 3, so $n - 1 > 1$. Therefore each factor $n-1, n+1$ has at least one prime number in its decomposition. It can't have two factors (necessarily equal to p and q), because none of $n-1, n+1$ is equal to 1. Therefore each of the two numbers $n-1, n+1$ is equal to one and only one of the primes p, q, therefore these two primes differ by ± 2.

Problem 6. *Draw the hyperbola*

$$\mathcal{H} : \{(x, y) \in \mathbb{R}^2 / x^2 - y^2 = 1\}.$$

Find all the points on $\mathcal{H}$ that have rational coordinates.

Hint: *Take the half-lines starting from $(-1, 0)$ and having a rational slope and see where they intersect the hyperbola.*

Answer. Claim: The points on the hyperbola with rational coordinates are exactly the points of intersection of the hyperbola with the lines $\mathcal{L}_t := \{y = t.(x+1)\}$, where $t \in \mathbb{Q}$.

If (x, y) is in $\mathcal{H} \cap \mathcal{L}_t$, then necessarily $x^2 = t^2(x+1)^2 + 1$, which is equivalent to

$$0 = (t^2 - 1)x^2 + 2t^2 x + t^2 + 1$$

Two cases: if $t = \pm 1$, then the only solution is $(x, y) = (-1, 0)$; if t is not in $\{-1, 1\}$ then the above equation is equivalent to $0 = (x+1).(x - \frac{t^2+1}{t^2-1})$, so besides $(-1, 0)$ there is only one other intersection point $(\frac{t^2+1}{t^2-1}, t.(1 + \frac{t^2+1.}{t^2-1}))$. Moreover, we see that if t is rational then this point has rational coordinates.

Therefore, we have a map $\mathbb{Q} - \{-1, 1\} \to \{\text{points of } \mathcal{H}\text{with rational coordinates}\}$ defined by associating to $\mathcal{L}_t$ the unique point of intersection with the hyperbola that is not $(-1, 0)$. By construction this map is injective (because a line is determined by 2 points!). It is also surjective, because the line joining $(-1, 0)$ to a point with rational coordinates has a rational slope, and this slope cannot be in $\{-1, 1\}$ (because the two lines through $(-1, 0)$ with those slopes do not have another intersection point with the hyperbola).

Math 311 — Correction of Homework 3

Problem 1. *Characterize the set of positive integers n such that* $\phi(2n) > \phi(n)$.

Answer. If n is odd then $\phi(2n) = \phi(2).\phi(n) = \phi(n)$. If n is even, it can be written as $n = 2^k.m$ with m odd. Thus $\phi(2n) = \phi(2^{k+1}.m) = \phi(2^{k+1}).\phi(m) = (2^{k+1} - 2^k).\phi(m) = 2.\phi(n) > \phi(n)$.Therefore the set of positive integers such that $\phi(2n) > \phi(n)$ coincides with the set of even integers.

Problem 2. *What are the last two digits, that is the tens and units digits of* $2^{1000}, 3^{1000}$*?*

Answer. For the first one, you can notice that $2^{12} \equiv -4(\mod 100)$ so $2^{12.12} \equiv 2^4$. Therefore $2^{1000} \equiv 2^{6.144+136} \equiv 2^{6.4}.2^{136} \equiv 2^{12.12+16} \equiv 2^4.2^{16} = 2^{12+8} \equiv (-4).2^8 \equiv -24 \equiv 76$ Therefore the last two digits are 76. For 3, things are much simpler: $3^{\phi(100)} \equiv 1$ so $3^{40} \equiv 1$. Thus $3^{1000} \equiv 3^{40.25} \equiv 1$, so the last digits are 01.

Problem 3. *Prove that for* $n \geq 2$ *the sum of all the positive integers less than n and coprime with n is* $\frac{n}{2}.\phi(n)$.

Answer. The answer I proposed to you was a bit long (you can still ask me if you tried it). Instead here is a simpler one, by one of you, Kevin Donahue. First, realize that $n/2$ is never coprime with n. Then if you pick any integer a coprime with n and less than $n/2$, the integer $n - a$ is coprime with n too and is between $n/2$ and n. Therefore the $\phi(n)$ integers that are coprime with n and less than n can be partitioned into two collections A and B with the same number of elements ($\phi(n)/2$), and each $a \in A$ can be paired with $n - a \in B$.Thus when you sum all of these pairs you get $n.\frac{\phi(n)}{2}$, which is the answer.

Problem 4. *Find all the primes p such that p divides* $2^p + 1$.

Answer. The prime 2 has not the property, so we can assume now that p is odd, but then Fermat's theorem implies that $2^p + 1 \equiv 3$ modulo p, therefore p must divide 3. Now 3 actually divides 9, so 3 is the only prime with this property.

Problem 5. *Show that* $x^2 - 2y^2 + 8z = 3$ *has no solutions* $(x, y, z) \in \mathbb{Z}^3$. (**Hint:** *reduce modulo 8).*

Answer. Clearly x must be odd (therefore congruent to $1, 3, 5, 7$ whose squares are all congruent to 1). So necessarily, $2y^2 \equiv -2$. But this is impossible because $2t^2$ only takes the values 0 or 2 modulo 8

Problem 6. *For any n show that* $\phi(n) = n.(1 - \frac{1}{p_1}) \dots (1 - \frac{1}{p_k})$ *where the* p_i *are the prime factors present in the prime decomposition of n.* (**Hint:**: *compute first* $\phi(p^s)$*, for any prime p.)*

Answer. First, $\phi(p^s) = p^s - p^{s-1} = p^s(1-\frac{1}{p})$ because the only integers less than p^s and not coprime to p^s are the multiples of p. Since we proved that $(G.C.D.(m,n) = 1 \Rightarrow \phi(m.n) = \phi(m).\phi(n))$, we can consider the decomposition of n in prime factors, $n = p_1^{r_1}.\dots.p_k^{r_k}$ and thus obtain

$$\phi(n) = \phi(p_1^{r_1}).\dots.\phi(p_k^{r_k}) = (p_1^{r_1}.(1-\frac{1}{p_1})).\dots.(p_k^{r_k}.(1-\frac{1}{p_k})).$$

Math 311 — Homework 4 due on Fr. 02/23

Problem 1. *Let R be a subring of the complex numbers $\mathbb{C}$ having the following two properties:*

1. *There is a disk D around the origin $0 \in \mathbb{C}$, such that $D \cap R = \{0\}$;*
2. *For any $z \in \mathbb{C}$ there exists an element $\lambda \in R$ such that $|z - \lambda| < 1$.*

   Show that any ideal I of R is the set of the multiples of an element $a \in R$.

   Hint*: Show that, in any ideal I of R, there exists one element $b \in I$ that is different from 0, and that is at minimal distance from the origin. Show that the ideal I coincides actually with the set of multiples of b (namely show that $I = b.R$).*

Answer. Pick any $r \in I$ different from the origin. If it is at minimal distance from the origin, then we are done. Otherwise, find one that is at strictly smaller distance from the origin. By continuing this process you get a sequence of decreasing positive real numbers. It has a limit l which is > 0 (because there is a small disk around the origin that contains only the element 0 in the ring). I claim that there is indeed an element $b \in I$ that is exactly at distance $|b| = l$ from the origin. If not I could find an infinite number of $a_i \in I$ with distance from the origin between l and $l + \epsilon$ (for an arbitrary ϵ. Among these a_i, two of them at least , say a_1, a_2 would be at distance less than 2ϵ. If you shift them to the origin (by substracting a_1, you would contradict the first condition. Now pick any $c \in I$. By the second condition, there exists $\lambda \in I$ such that $|\frac{c}{b} - \lambda| < 1$. But this implies $|c - \lambda.b| < |b|$. By the definition of b this implies that necessarily $c = \lambda.b$, and we are done: the ideal I is the set of multiples of the element b.

Problem 2. *Let p be an odd prime and let $d = b^2 - 4ac$. Show that the congruence*

$$ax^2 + bx + c \equiv 0 \ (mod\ p)$$

is equivalent to the congruence $y^2 \equiv d\ (mod\ p)$, where $y = 2ax + b$. Conclude that if $d \equiv 0\ (mod\ p)$, then there is exactly one solution modulo p; if d has a square root in $\mathbb{Z}/p\mathbb{Z}$, then there are two (non congruent) solutions; and if d has no square root in $\mathbb{Z}/p\mathbb{Z}$, then there are no solutions. What about the case $p = 2$?

Answer. Here I should have said: "assume that a is not zero", otherwise the question is not correct. We have $y^2 - d \equiv 4a^2.x^2 + 4a.b.x + b^2 - b^2 + 4.a.c \equiv 4a.(a.x^2 + b.x + c) \equiv 0$. Therefore $a.x^2 + b.x + c \equiv 0$ implies $y^2 - d \equiv 0$. Conversely: if $y^2 - d \equiv 0$ then $4a.(a.x^2 + b.x + c) \equiv 0$. Since p is odd and a is not zero, this implies the first condition. Now if $d \equiv 0$, then necessarily $y \equiv 0$ and there is only one solution $x = (-b).(2a)^{-1}$.If d has a square root y, then $-y$ is the only other solution to $y^2 \equiv d$, and we get two solutions $x = (2a)^{-1}(\pm y - b)$. If d has no square root then the initial equation has no solution. For $p = 2$: the equation is equivalent to $(a + b).x \equiv -c$ and this has a unique solution if and only if $(a + b)$ is not zero.

Problem 3. *Consider $\mathbb{Z}[X]$, the set of polynomials with coefficients in $\mathbb{Z}$. Show that there are ideals in $\mathbb{Z}[X]$ that cannot be written as the set of multiples of a single polynomial.*

Hint*: consider the ideal generated by* 2 *and* X *(meaning: the ideal made of all the possible sums of one multiple of* 2 *and one multiple of* X*).*

Answer. Consider the ideal I made of all the polynomials that can be written as $2k + X.Q(X)$. Assume $I = P(X).\mathbb{Z}[X]$. Since $2 \in I$ we see that P must be of degree 0, so it is a constant a. Now $X \in I$ so we must have $X = a.bX$ for some $b \in \mathbb{Z}$. Therefore we must have $a = \pm 1$ and then $I = \mathbb{Z}[X]$. But clearly 3 is not in I so there is a contradiction.

Problem 4. *Go on the web and find a short description of the "ElGamal cryptosystem". Write a short (*< 10 *lines) description of this algorithm used for encryption.*

Answer. See for example this article: http://en.wikipedia.org/wiki/Elgamal

Problem 5. *Let p be an odd prime. Assume that in $\mathbb{Z}/p\mathbb{Z}$ there exists a nonzero element ζ such that*

- *ζ has no square root in $\mathbb{Z}/p\mathbb{Z}$;*
- *the order of ζ in the multiplicative group of $\mathbb{Z}/p\mathbb{Z}$ is exactly* 4.

  Show that 2 *has no square root in $\mathbb{Z}/p\mathbb{Z}$.*

Answer. Since ζ is of order exactly 4, we know that $\zeta^2 \equiv -1$. This implies $(\zeta + 1)^2 \equiv 2.\zeta$. If 2 had a square root x (meaning $x^2 \equiv 2$, then you would have $\zeta \equiv (\zeta + 1)^2.(x^{-1})^2$ (a square), but this is a contradiction.

Math 311 — Homework 5 due on Fr. 03/02

The R.S.A system. For the following problems, the same notations will be kept. First, the sender takes two large primes p, q, and forms $n = p.q$.He also picks an integer e such that e and $\phi(n)$ are coprime.The message to be sent is an integer P (less than n, and coprime with n). The encrypted message C is given by $C \equiv P^e$ mod n . At this point, p, q are only known to the sender, but n, e, C are public. Now the recipient of the message has a key, that is not public: the key d is an integer such that $d.e \equiv 1 \bmod \phi(n)$, or equivalently such that $e.d = k.\phi(n) + 1$, for some k. Now deciphering the encrypted message C is easy: the recipient of the message just needs to perform $C^d \equiv P^{e.d} \equiv P^{\phi(n).k}.P \equiv P$ mod n , thanks to Fermat's theorem. For these problems, you need also to remember than factorizing a large number is really hard, but finding a G.C.D. is not...

Problem 1. *Show that if the message P is not coprime with n, then just knowing* $C = P^e$ *and n, one can recover* p, q*. If both* p, q *have 100 digits, what is the probability of producing such a message P that is not coprime with n?*

Problem 2. *Suppose that you have two groups of recipients. Both of them use the same number n, but use two different exponents* e_1, e_2 *such that* $G.C.D.(e_1, e_2) = 1$*.Assume that the same message P is sent to the two groups. Therefore you have two public crypted messages* $C_1 \equiv P^{e_1}$ *and* $C_2 \equiv P^{e_2}$*. Show that knowing these two encrypted messages one can recover the initial message P.*

Problem 3. *Here we suppose that we have three senders, using different integers* n_1, n_2, n_3*, but using the same exponent* $e_1 = e_2 = e_3 = 3$*. Show that if these three senders encrypt the same message P (thus producing three public crypted messages* $C_i \equiv P^3 \bmod n_i$*), then one can recover the initial message P.*

Problem 4. *Assume you are a bit paranoid and you encrypt your message P using* n, e_1 *to produce* $C = P^{e_1} \bmod n$ *, and then encrypt one more time, using* n, e_2 *(same n) to produce the final (public) crypted message* $D = C^{e_2} \bmod n$ *.Show that in reality you will not gain much by doing this.*

Problem 5. *Read the proof of the quadratic reciprocity that I gave on the web page.Ask me (at least) one question about it in class next week.*

The R.S.A system.

Problem 1. *Show that if the message P is not coprime with n, then just knowing $C = P^e$ and n, one can recover p, q. If both p, q have 100 digits, what is the probability of producing such a message P that is not coprime with n?*

Answer. If the message P is not coprime with n, then it must be a multiple of one of the prime factors, say p. Since the message is smaller than n it can't be a multiple of n. Thus $G.C.D.(n, P^e) = p$, and therefore we can retrieve the factors of n. There are $\phi(n) = n.(1 - \frac{1}{p}).(1 - \frac{1}{q})$ integers coprime with n and less than n so the probability of being coprime with n is $\frac{\phi(n)}{n} = (1 - \frac{1}{p}).(1 - \frac{1}{q}) \simeq 1 - \frac{2}{10^{100}}$, and the probability of not being coprime is really low (of order $\frac{2}{10^{100}}$).

Problem 2. *Suppose that you have two groups of recipients. Both of them use the same number n, but use two different exponents e_1, e_2 such that $G.C.D.(e_1, e_2) = 1$.Assume that the same message P is sent to the two groups. Therefore you have two public crypted messages $C_1 \equiv P^{e_1}$ and $C_2 \equiv P^{e_2}$. Show that knowing these two encrypted messages one can recover the initial message P.*

Answer. Since $G.C.D.(e_1, e_2) = 1$ we know the existence of integers a, b such that $ae_1 + be_2 = 1$. We can assume $a > 0$ and $b < 0$, therefore $ae_1 = 1 - be_2$ (equality between positive integers). But now $C_1^a = P^{ae_1} = P.P^{e_2.(-b)} = P.C_2^{-b}$, so we can find P, because C_1, C_2 are known.

Problem 3. *Here we suppose that we have three senders, using different integers n_1, n_2, n_3, but using the same exponent $e_1 = e_2 = e_3 = 3$. Show that if these three senders encrypt the same message P (thus producing three public crypted messages $C_i \equiv P^3$ mod n_i), then one can recover the initial message P.*

Answer.

- If one of the pairs (n_i, n_j) is not made of coprime integers, then we can easily compute the G.C.D. of the pair which would be one factor in the factorisation of n_i (and therefore we would be done);
- We assume now that all the pairs are coprime: we can apply the chinese remainder theorem which says that the following map is an isomorphism

$$\mathbb{Z}/n_1n_2n_3 \to \mathbb{Z}/n_1 \times \mathbb{Z}/n_2 \times \mathbb{Z}/n_3$$

  and therefore one can find an integer C such that $C \mapsto (C_1, C_2, C_3) = (P^3, P^3, P^3)$, therefore $C \equiv P^3 \bmod n_1n_2n_3$. But since P^3 is an integer less than $n_1n_2n_3$, we can simply compute its cubic root (as a real number!), and get the answer.

Problem 4. *Assume you are a bit paranoid and you encrypt your message P using n, e_1 to produce $C = P^{e_1}$ mod n , and then encrypt one more time, using n, e_2 (same n) to produce the final (public) crypted message $D = C^{e_2}$ mod n .Show that in reality you will not gain much by doing this.*

Answer. If you encrypt twice, your crypted message becomes $(P^{e_1})^{e_2}$ mod n. So it is the same as using (n, e_1e_2) for the encryption. But now the problem of finding an inverse of e_1e_2 mod $\phi(n)$ has exactly the same difficulty as the problem of finding an inverse for e_1, e_2.

Problem 5. *Read the proof of the quadratic reciprocity that I gave on the web page.Ask me (at least) one question about it in class next week.*

"Is it on the test?"

Math 311 **Homework 6 due on Monday 03/19**

Problem 1. *Let $\tau(n)$ be equal to the number of divisors of n. Show that $\tau(m.n) = \tau(m).\tau(n)$ if m and n are coprime.*

Problem 2. *Is the ring $\mathbb{Z}[X]$ a euclidian ring? Is it a Principal Ideal Domain?*

Problem 3. *Show that $\mathbb{Q}[\sqrt{-5}]$ (which is by definition $\{a + b(i\sqrt{5}) \mid a, b \in \mathbb{Q}\}$) is isomorphic to $\mathbb{Q}[X]/(X^2 + 5)$.*

Problem 4. *Show that if p is prime and a is an integer not divisible by p, then there exists integers x and y such that $a.x \equiv y$ (mod p) , with $0 < |x| < \sqrt{p}$ and $0 < |y| < \sqrt{p}$.*

*(**Hint:** consider all the integers of the form $au - v$ with $0 \leq u \leq [\sqrt{p}]$, $0 \leq v \leq [\sqrt{p}]$ where $[.]$ denotes the integer part, and show that there must be two of them that are congruent modulo p, then form the difference of these two integers).*

Problem 5. *In order to do this problem you need the results of the previous exercise. One would like to know whether a prime integer like 3, stays a prime when we pass from $\mathbb{Z}$ to the Gaussian integers $\mathbb{Z}[i]$. In other words, can we have a non trivial factorization $3 = (a + bi).(c + di)$? By taking the square of the modulus, one finds $3 = (a^2 + b^2).(c^2 + d^2)$. Therefore one is reduced to the problem of determining when a prime integer is the sum of two squares.*

1. *Show that if a prime number $p \neq 2$ can be written as a sum $a^2 + b^2$ then necessarily one has $p \equiv 1($ mod 4 $)$.*

2. *Explain why (-1) has a square root in $\mathbb{Z}/p\mathbb{Z}$, when p is a prime of the form $4n + 1$.*

3. *Use the previous question together with the previous problem to show that if p prime is congruent to 1 modulo 4, then p can be written as the sum of two squares.*

4. *If $p \equiv 1$ (mod 4) then show that p can be written as a product of two elements in $\mathbb{Z}[i]$ that are not invertible.(Hence we proved that such a prime p is not anymore a prime in $\mathbb{Z}[i]\ldots$)*

Problem 1. *Let $\tau(n)$ be equal to the number of divisors of n. Show that $\tau(m.n) = \tau(m).\tau(n)$ if m and n are coprime.*

Answer. See the correction of the midterm, where we proved that all the products $a.b$ where a divides m and b divides n coincide exactly with the set of divisors of $m.n$ when m, n are coprime.

Problem 2. *Is the ring $\mathbb{Z}[X]$ a euclidian ring? Is it a Principal Ideal Domain?*

Answer. In some previous HW, we proved that the ideal generated by 2 and X is not principal, therefore our ring is not a principal ideal domain, and therefore it isn't a euclidian ring either.

Problem 3. *Show that $\mathbb{Q}[\sqrt{-5}]$ (which is by definition $\{a + b(i\sqrt{5}) \mid a, b \in \mathbb{Q}\}$) is isomorphic to $\mathbb{Q}[X]/(X^2+5)$.*

Answer. Consider the surjective map $\phi : \mathbb{Q}[X] \longrightarrow \mathbb{Q}[\sqrt{-5}]$ given by $P(X) \mapsto P(i.\sqrt{5})$. We know that $\mathbb{Q}[X]/ker\phi$ is isomorphic to $im\phi = \mathbb{Q}[\sqrt{-5}]$, so we have to prove that $ker\phi = (X^2+5).\mathbb{Q}[X]$. One inclusion is easy: if a polynomial $R(X)$ is a multiple of X^2+5, then $P(i.\sqrt{5}) = 0$. Conversely, take $S(X)$ in ker ϕ, then write the euclidian division of this polynomial by X^2+5: $S(X) = (X^2+5).R(X) + bX + a$. Since $S(X)$ is in ker ϕ, one must have $b(i\sqrt{5}) + a = 0$, but this implies $b = a = 0$ and therefore $S(X)$ must be a multiple of X^2+5.

Problem 4. *Show that if p is prime and a is an integer not divisible by p, then there exists integers x and y such that $a.x \equiv y$ (mod p) , with $0 < |x| < \sqrt{p}$ and $0 < |y| < \sqrt{p}$.*

*(**Hint:** consider all the integers of the form $au - v$ with $0 \leq u \leq [\sqrt{p}]$, $0 \leq v \leq [\sqrt{p}]$ where $[.]$ denotes the integer part, and show that there must be two of them that are congruent modulo p, then form the difference of these two integers).*

Answer. Since each of u, v can take $[\sqrt{p}] + 1 > \sqrt{p}$ values, there exist at least $p = \sqrt{p}.\sqrt{p}$ integers of the form $au - v$. But there are only p possible values modulo p, therefore two at least of these integers must be congruent modulo p, say $au - v \equiv au' - v'$. But then $ax \equiv y$ if one writes $x = u - u', y = v - v'$.Now x,y satisfy $0 \leq |x| < \sqrt{p}$ and $0 \leq |y| < \sqrt{p}$. If one of them is zero, then the other one must be zero modulo p, and therefore must be zero in $\mathbb{Z}$ (because 0 is the only multiple of zero in this range of possible values for x, y).

Problem 5. *In order to do this problem you need the results of the previous exercise. One would like to know whether a prime integer like 3, stays a prime when we pass from $\mathbb{Z}$ to the Gaussian integers $\mathbb{Z}[i]$. In other words, can we have a non trivial factorization $3 = (a + bi).(c + di)$? By taking the square of the modulus, one finds $3 = (a^2 + b^2).(c^2 + d^2)$. Therefore one is reduced to the problem of determining when a prime integer is the sum of two squares.*

Math 311 Homework 6 due on Monday 03/19

1. *Show that if a prime number $p \neq 2$ can be written as a sum $a^2 + b^2$ then necessarily one has $p \equiv 1($ mod 4 $)$.*

2. *Explain why (-1) has a square root in $\mathbb{Z}/p\mathbb{Z}$, when p is a prime of the form $4n + 1$.*

3. *Use the previous question together with the previous problem to show that if p prime is congruent to 1 modulo 4, then p can be written as the sum of two squares.*

4. *If $p \equiv 1$ (mod 4) then show that p can be written as a product of two elements in $\mathbb{Z}[i]$ that are not invertible.(Hence we proved that such a prime p is not anymore a prime in $\mathbb{Z}[i] \ldots$)*

Answer.

1. The only possible values taken by squares modulo 4 are 0 and 1. So sums of two squares can only take the values $0, 1, 2$, and never 3.(Remember that an odd prime is congruent to 1 or 3 modulo 4).

2. When we studied quadratic reciprocity we proved that -1 is a square modulo p if and only if $\frac{p-1}{2}$ is even.

3. From the previous question, we know the existence of an integer a with square $\equiv -1$ modulo p. From the previous exercise we know the existence of x, y such that $a.x \equiv y$ and $0 < |x| < \sqrt{p}$ and $0 < |y| < \sqrt{p}$. But this implies $-x^2 \equiv a^2x^2 \equiv y^2$, so p divides $0 < x^2 + y^2 < 2p$, therefore $x^2 + y^2$ must be p and we are done.

4. Just notice that $p = x^2 + y^2 = (x + iy).(x - iy)$, and that none of $x + iy, x - iy$ is invertible because $|x \pm iy| = p$, and we know that invertible elements must have a norm equal to 1.

Math 311 Homework 7 due on Monday 03/26

Problem 1. *Consider the map* $f : \mathbb{Z}[X] \to \mathbb{Z} \times \mathbb{Z}$, *given by* $P(X) \mapsto (P(1), P(2))$. *Is it a surjective map? What is the kernel of it?*

Problem 2. *As in the class, given a ring* R, *we define* $SpecR$ *as the set of all prime ideals of* R, *distinct from* R *itself.* $SpecR$ *is a topological space, once we define the closed sets as follows: the closed sets are all the sets of prime ideals of the form* $V(I)$, *where* I *is an ideal and* $V(I)$ *is the set of all prime ideals in* $SpecR$ *that contain* I.

1. *show that if* $Z_1 = V(I_1), Z_2 = V(I_2)$ *are two closed sets, then* $Z_1 \cap Z_2 = V(I_1 + I_2)$ *and* $Z_1 \cup Z_2 = V(I_1 \cap I_2)$;
2. *prove that the intersection of any collection of closed sets* Z_i *is still a closed set.*

Problem 3. *Let* A *be a ring and* I, J *two ideals in* A. *Let's write the "reduction map"* $\rho : A \longrightarrow A/I$ *that takes any* $a \in A$ *and returns* $a mod I$ *(it can be written as* $\bar{a}$ *if you prefer).*

1. *Show that* $\rho(J)$ *is an ideal in* A/I.
2. *Show that* $A/(I + J)$ *is isomorphic to* $(A/I)/(\rho(J))$.
3. *Application: show that* $\mathbb{Z}[X]/((3) + (X^2 + 5))$ *is isomorphic to* $(\mathbb{Z}/3\mathbb{Z})[\sqrt{-5}]$.

Math 311 Correction of HW7

Problem 1. *Consider the map $f : \mathbb{Z}[X] \to \mathbb{Z} \times \mathbb{Z}$, given by $P(X) \mapsto (P(1), P(2))$. Is it a surjective map? What is the kernel of it?*

Answer. The map is clearly surjective: if you pick any $(a, b) \in \mathbb{Z} \times \mathbb{Z}$, then one preimage is $P(X) = b(X-1) - a(X-2)$. The map is certainly not injective: for example $S(X) = (X-1)(X-2)$ is in the kernel. Let's find the kernel: by euclidian division, one can write: $P(X) = (X-1)(X-2).Q(X) + aX + b$ for any polynomial $P(X) \in \mathbb{Z}[X]$.But one can do more, actually $aX + b = P(2)(X-1) - P(1)(X-2)$ (just notice that $P(1) = a + b, P(2) = 2a + b$). Therefore immediately one knows that $ker f$ is the principal ideal generated by $(X-1)(X-2)$.

Problem 2. *As in the class, given a ring R, we define $SpecR$ as the set of all prime ideals of R, distinct from R itself. $SpecR$ is a topological space, once we define the closed sets as follows: the closed sets are all the sets of prime ideals of the form $V(I)$, where I is an ideal and $V(I)$ is the set of all prime ideals in $SpecR$ that contain I.*

1. *show that if $Z_1 = V(I_1), Z_2 = V(I_2)$ are two closed sets, then $Z_1 \cap Z_2 = V(I_1 + I_2)$ and $Z_1 \cup Z_2 = V(I_1 \cap I_2)$;*
2. *prove that the intersection of any collection of closed sets Z_i is still a closed set.*

Answer.

1. If a prime ideal $\mathcal{P}$ is in $Z_1 \cap Z_2$, then it contains both I and J, hence it contains their sum $I + J$, hence it is in $V(I + J)$. Conversely a prime ideal containing the sum must contain each of the two ideals. Now if $\mathcal{P}$ is in $Z_1 \cup Z_2$ then it contains either I_1 or I_2, and in both cases it contains $I_1 \cap I_2$, so it is in $V(I_1 \cap I_2)$. Now assume that you have a proper prime ideal $\mathcal{P}$ in $V(I_1 \cap I_2)$: then either it contains I_1 (and then we are done because $\mathcal{P}$ will be in $V(I_1) \cup V(I_2)$), or it doesn't contain I_1, therefore there exists $i \in I_1$ that is not in $\mathcal{P}$. Now pick any $j \in I_2$: the product $i.j \in I_1 \cap I_2$, so it is in $\mathcal{P}$, but this ideal is prime and doesn't contain i, therefore it must contain j, for any $j \in I_2$ hence $\mathcal{P}$ contains I_2 and we are done.
2. The same argument works for any family of ideals: the intersection of any family of $V(I_\alpha)$ is simply $V(\sum_\alpha I_\alpha)$, where the sum of any family of ideals is defined as the set of all finite sums of elements taken in these ideals.

Problem 3. *Let A be a ring and I, J two ideals in A. Let's write the "reduction map" $\rho : A \longrightarrow A/I$ that takes any $a \in A$ and returns $a \bmod I$ (it can be written as $\bar{a}$ if you prefer).*

1. *Show that $\rho(J)$ is an ideal in A/I.*
2. *Show that $A/(I+J)$ is isomorphic to $(A/I)/(\rho(J))$.*
3. *Application: show that $\mathbb{Z}[X]/((3)+(X^2+5))$ is isomorphic to $(\mathbb{Z}/3\mathbb{Z})[\sqrt{-5}]$.*

Answer.

1. We can notice that $\rho(J)$ is just J mod I: it's clearly an additive group (because $\overline{j_1} + \overline{j_2} = \overline{j_1 + j_2}$) and if you multiply any $\overline{j}$ by $\overline{a}$ (where a is any element of A), then you get $\overline{a.j}$ which is in $\rho(J)$ because J is an ideal and therefore $a.j \in J$.
2. Consider the map $A \to A/I \to (A/I)/(\rho(J))$.It is surjective (composition of two surjective maps). What about the kernel? Well the kernel is the set of all elements $a \in A$ such that a mod $I = j$ mod I for some $j \in J$, but this means that $a - j \in I$ so $a - j = i$ for some $i \in I$, or if you prefer $a = i + j$. Thus the kernel of the map is included in $I + J$. Conversely $I + J$ is in the kernel. By the isomorphism theorem we know that $A/(I+J)$ is then isomorphic to $(A/I)/(\rho(J))$.
3. Application: replace I by (3) and J by $(X^2 + 5)$.

Math 311 **Homework 8 due on Wed. 04/18**

Problem 1. *Expand in continued fractions the following rational numbers:* $\frac{67}{41}$, $\frac{111}{19}$.

Problem 2. *We write a continued fraction* $a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \dots}}$ *as* $\langle a_0, a_1, \dots \rangle$. *You can truncate the continued fraction in order to get* $\langle a_0, a_1, \dots, a_n \rangle$ *and reduce the result to a fraction* $r_n = \frac{p_n}{q_n}$. *For* $n \geq 1$, *prove that* $\frac{q_{n+1}}{q_n} = \langle a_n, a_{n-1}, \dots, a_2, a_1 \rangle$. *Find and prove a similar continued fraction expansion for* $\frac{p_n}{p_{n-1}}$, *assuming* $a_0 \geq 0$.

Problem 3. *Let* u_0/u_1 *be a rational number in its lowest terms, and write* $u_0/u_1 = \langle a_0, a_1, \dots, a_n \rangle$. *Show that if* $0 \leq i < n$, *then* $|r_i - u_0/u_1| \leq 1/(q_i q_{i+1})$, *with equality if and only if* $i = n - 1$.*(Here* $r_i = p_i/q_i$ *is the truncated fraction equal to* $\langle a_0, a_1, \dots, a_i \rangle$*).*

Problem 4 (Geometric interpretation of the denominators q_n)**.** *For an irrational number* ζ *(this greek letter is called "zeta"), consider the point on the unit circle* $\lambda = e^{2\pi i \zeta}$ *(this greek letter is called "lambda").We study the orbit* $1 \mapsto \lambda \mapsto \lambda^2 \mapsto \dots$ *under the rotation* $z \mapsto \lambda z$ *of the circle. We say that a point* λ^q *on this orbit is a* **closest return** *to* 1 *if*

$$|\lambda^q - 1| < |\lambda^m - 1|$$

for every m *with* $0 < m < q$, *so that* λ^q *is closer to* 1 *than any preceding point on the orbit.*

Show that the point $\lambda^q = e^{2\pi i \zeta q}$ *is a closest return to* 1 *along the orbit*

$$1 \mapsto \lambda \mapsto \lambda^2 \mapsto \dots$$

if and only if q *is one of the denominators* $1 = q_1 \leq q_2 < q_3, \dots$ *in the continued fraction approximations to* ζ. *Furthermore, if* $q = q_n$ *with* $n \geq 2$ *then the order of magnitude of the distance* $|\lambda^q - 1|$ *is given by*

$$\frac{2}{q_{n+1}} < |\lambda^{q_n} - 1| < \frac{2\pi}{q_{n+1}}$$

Some hints for that*: prove that* $|\lambda^m - 1| = 2\sin(\pi << m\zeta >>)$, *where* $<< x >>$ *represents* $min|x + n|, n \in \mathbb{Z}$ *(the distance from the point* x *to the closest integer).Then use the fact that* $4 < 2\sin(\pi t)/t < 2\pi$ *for* $t \in (0, 1/2)$. *Also notice that* $q_n \zeta \equiv x_n$ *mod* $\mathbb{Z}$, *and remember that we proved that* $|x_n| < 1/2$ *for* n *larger than 2.*

Problem 1. *Expand in continued fractions the following rational numbers:* $\frac{67}{41}, \frac{111}{19}$.

Answer. You will find $67/41 = \langle 1,1,1,1,2,1,3\rangle$ and $111/19 = \langle 5,1,5,3\rangle$.

Problem 2. *We write a continued fraction* $a_0 + \frac{1}{a_1+\frac{1}{a_2+\dots}}$ *as* $\langle a_0, a_1, \dots\rangle$. *You can truncate the continued fraction in order to get* $\langle a_0, a_1, \dots, a_n\rangle$ *and reduce the result to a fraction* $r_n = \frac{p_n}{q_n}$. *For* $n \geq 1$, *prove that* $\frac{q_n}{q_{n-1}} = \langle a_n, a_{n-1}, \dots, a_2, a_1\rangle$. *Find and prove a similar continued fraction expansion for* $\frac{p_n}{p_{n-1}}$, *assuming* $a_0 \geq 0$.

Answer. Prove it by induction:

1. For $n = 1$, one has $q_0 = 1, q_1 = a_1$ so one gets $q_1/q_0 = a_1$;
2. Assume the result is true for n: then one has $\langle a_{n+1}, a_n, \dots, a_2, a_1\rangle = a_{n+1} + \dfrac{1}{\langle a_n, \dots, a_2, a_1\rangle} = a_{n+1} + q_{n-1}/q_n = \frac{a_{n+1}q_n+q_{n-1}}{q_n} = \frac{q_{n+1}}{q_n}$ (remember how we get the expansion using Euclid's algorithm). A similar proof will show that $p_n/p_{n-1} = \langle a_n, \dots, a_1, a_0\rangle$.

Problem 3. *Let* u_0/u_1 *be a rational number in its lowest terms, and write* $u_0/u_1 = \langle a_0, a_1, \dots, a_n\rangle$. *Show that if* $0 \leq i < n$, *then* $|r_i - u_0/u_1| \leq 1/(q_i q_{i+1})$, *with equality if and only if* $i = n-1$.*(Here* $r_i = p_i/q_i$ *is the truncated fraction equal to* $\langle a_0, a_1, \dots, a_i\rangle$*).*

Answer. The inequality has been proved in class. Now if $i = n-1$, one has $|\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}}| = \frac{1}{q_n q_{n-1}}$ because we know that $p_n q_{n-1} - p_{n-1} q_n = \pm 1$.

Assume now that one has equality: since we know that the even terms p_{2k}/q_{2k} are strictly increasing towards the limit p_n/q_n, that the odd terms strictly decrease, and that the difference between consecutive terms is $\pm 1/q_i q_{i+1}$, we deduce that the equality is possible only when the initial fraction is exactly one of the approximants (and this happens only with the last one).

Problem 4 (Geometric interpretation of the denominators q_n)**.** *For an irrational number* ζ *(this greek letter is called "zeta"), consider the point on the unit circle* $\lambda = e^{2\pi i\zeta}$ *(this greek letter is called "lambda").We study the orbit* $1 \mapsto \lambda \mapsto \lambda^2 \mapsto \dots$ *under the rotation* $z \mapsto \lambda z$ *of the circle. We say that a point* λ^q *on this orbit is a* **closest return** *to* 1 *if*

$$|\lambda^q - 1| < |\lambda^m - 1|$$

for every m *with* $0 < m < q$, *so that* λ^q *is closer to* 1 *than any preceding point on the orbit.*

Show that the point $\lambda^q = e^{2\pi i\zeta q}$ *is a closest return to* 1 *along the orbit*

$$1 \mapsto \lambda \mapsto \lambda^2 \mapsto \dots$$

if and only if q is one of the denominators $1 = q_1 \leq q_2 < q_3, \ldots$ in the continued fraction approximations to ζ. Furthermore, if $q = q_n$ with $n \geq 2$ then the order of magnitude of the distance $|\lambda^q - 1|$ is given by

$$\frac{2}{q_{n+1}} < |\lambda^{q_n} - 1| < \frac{2\pi}{q_{n+1}}$$

Answer. As in the class, let's prove that a best approximation to ζ is necessarily of the form p_n/q_n, and that for $n \geq 1$, q_n is the smallest integer $q > q_{n-1}$ such that $\|q\zeta\| < \|q_{n-1}\zeta\|$. Let's consider a/b a best approximation to ζ.

First, suppose $a/b < p_0/q_0 = a_0/1$, then $|\zeta - a_0| < |\zeta - a/b| \leq |b\zeta - a|$ (contradiction with the fact that a/b is a best approximation). Second, suppose $a/b > p_1/q_1$, then $|a/b - \zeta| > |a/b - p_1/q_1| \geq \frac{1}{bq_1}$ and therefore one would have $|b\zeta - a| > \frac{1}{q_1} = \frac{1}{a_1} \geq |\zeta - a_0|$. (contradiction). Finally assume that a/b is strictly between $\frac{p_{n-1}}{q_{n-1}}$ and $\frac{p_{n+1}}{q_{n+1}}$, then

$$\frac{1}{bq_{n-1}} \leq |\frac{a}{b} - \frac{p_{n-1}}{q_{n-1}}| < |\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}}| = \frac{1}{q_n q_{n-1}},$$

from which we deduce that $q_n < b$. On the other hand we know that

$$\frac{1}{bq_{n+1}} \leq |\frac{a}{b} - \frac{p_{n+1}}{q_{n+1}}| \leq |\zeta - \frac{a}{b}|,$$

which implies

$$|q_n\zeta - p_n| < \frac{1}{q_{n+1}} \leq |b\zeta - a|,$$

and together with $q_n < b$, this is a contradiction to the fact that a/b is a best approximation.

Now let's prove by induction on n the second part of the theorem (that q_n is the smallest integer $q > q_{n-1}$ such that $\|q\zeta\| < \|q_{n-1}\zeta\|$):

For $n = 0$, there is nothing to prove (because $q_0 = 1$), assume the property is true for $n \geq 0$. Let q be the smallest integer $> q_n$ such that $\|q\zeta\| < \|q_n\zeta\|$ and let p be such that $\|q\zeta\| = |q\zeta - p|$. Then by induction p_n/q_n is a best approximation, so p/q is also a best approximation., therefore it must be of the form $p_{n'}/q_{n'}$, but q is chosen as the smallest such that $\|q\zeta\| < \|q_n\zeta\|$, so $q = q_{n+1}$, and then automatically $p = p_{n+1}$ and we are done.

Math 311 Homework 9 due on Fr 04/27

Problem 1. *Expand in continued fraction $\sqrt{2}$ and $\sqrt{15}$.*

Problem 2. Diophantine conditions

Given some fixed real number $k \geq 2$, let us say that an irrational number ζ satisfies a Diophantine condition of order k if there is some $\epsilon > 0$ (depending on ζ) so that

$$|\zeta - \frac{p}{q}| > \frac{\epsilon}{q^k},$$

for every rational number $\frac{p}{q}$.We write D_k the set of all irrational numbers ζ which satisfy such a condition.

Now let f be a polynomial of degree d with integer coefficients, and suppose that $f(\alpha) = 0$ where α is irrational. If every other root of this equation has distance at least ϵ from α, and if $|f'(x)| < K$ in the open interval $(\alpha - \epsilon, \alpha + \epsilon)$, show that

$$K.|\alpha - p/q| \geq |f(p/q)| \geq 1/q^d$$

for every rational number p/q in $(\alpha - \epsilon, \alpha + \epsilon)$. Conclude that $\alpha \in D_d$, and hence that all irrational numbers in the complement of the union of all the D_d are transcendental (this means that they cannot be roots of a polynomial with integer coeffients).

Problem 3. *Example of transcendental numbers:(due to Liouville). Show that the number*

$$\alpha = \sum_{n=0}^{\infty} \frac{1}{10^{n!}}$$

is transcendental.

Hint: *Look at the partial sum $\frac{p_k}{q_k} = \sum_{n=0}^{\infty} \frac{1}{10^{n!}}$, with $q_k = 10^{k!}$. Then try to find a constant S such that $|\alpha - \frac{p_k}{q_k}| \leq \frac{S}{q_k^{k+1}}$. Conclude with the previous problem.*

Problem 4. *Find two rational numbers a/b such that*

$$|\sqrt{2} - \frac{a}{b}| < \frac{1}{\sqrt{5}b^2}.$$

Math 311 Homework 9 due on Fr 04/27

Problem 1. *Expand in continued fraction $\sqrt{2}$ and $\sqrt{15}$.*

Answer. For $sqrt2$, just notice that it is the solution of $(x-1).(x+1) = 1$, so it satisfies $x = 1 + \frac{1}{1+x}$. So if you plug again x in this you get the expansion $1 + \frac{1}{2+\frac{1}{2+\dots}}$. For $sqrt15 = 3.87298\dots$, one possible thing is to expand it from its decimal expansion, and then realize that there is a pattern, namely that $x = 3 + \frac{1}{1+\frac{1}{6+\frac{1}{1+1/6\dots}}}$. Then you need to verify the pattern you found: set $y = x - 3$, and verify that $y = \frac{1}{1+\frac{1}{6+y}}$.

Problem 2. Diophantine conditions

Given some fixed real number $k \geq 2$, let us say that an irrational number ζ satisfies a Diophantine condition of order k if there is some $\epsilon > 0$ (depending on ζ) so that

$$|\zeta - \frac{p}{q}| > \frac{\epsilon}{q^k},$$

for every rational number $\frac{p}{q}$.We write D_k the set of all irrational numbers ζ which satisfy such a condition.

Now let f be a polynomial of degree d with integer coefficients, and suppose that $f(\alpha) = 0$ where α is irrational. If every other root of this equation has distance at least ϵ from α, and if $|f'(x)| < K$ in the open interval $(\alpha - \epsilon, \alpha + \epsilon)$, show that

$$K.|\alpha - p/q| \geq |f(p/q)| \geq 1/q^d$$

for every rational number p/q in $(\alpha - \epsilon, \alpha + \epsilon)$. Conclude that $\alpha \in D_d$, and hence that all irrational numbers in the complement of the union of all the D_d are transcendental (this means that they cannot be roots of a polynomial with integer coeffients).

Answer. Let's write $f(x) = a_d x^d + \dots + a_0$ First, one notices that if $p/q \in (\alpha - \epsilon, \alpha + \epsilon)$ then it's not a root of $f(x)$ and one has $f(p/q) = a_d(p/q)^d + \dots + a_0 = \frac{\text{nonzero integer}}{q^d}$ so the absolute value is $\geq 1/q^d$. Now using calculus, we know that $|f(p/q)| = |f(\alpha) - f(p/q)| = |f'(c)|.|\alpha - p/q|$ for some c between α and p/q. But we know that for such a c, one has $|f'(c)| < K$. An immediate consequence is that $\alpha \in D_d$. Now an irrational number that is not in any of the D_d cannot be a root of a polynomial with integer coefficients, and hence it is transcendental (by definition).

Problem 3. *Example of transcendental numbers:(due to Liouville). Show that the number*

$$\alpha = \sum_{n=0}^{\infty} \frac{1}{10^{n!}}$$

is transcendental.

Hint: *Look at the partial sum $\frac{p_k}{q_k} = \sum_{n=0}^{k} \frac{1}{10^{n!}}$, with $q_k = 10^{k!}$. Then try to find a constant S such that $|\alpha - \frac{p_k}{q_k}| \leq \frac{S}{q_k^{k+1}}$. Conclude with the previous problem.*

Answer. One has $|\alpha - \frac{p_k}{q_k}| = |\frac{1}{10^{(k+1)!}} + \frac{1}{10^{(k+2)!}} + \ldots| < \frac{1}{10^{(k+1)!}}.(1 + \frac{1}{10} + \frac{1}{10^2} + \ldots) = \frac{1}{10^{(k+1)!}}.\frac{10}{9} = \frac{S}{q_k^{k+1}}$ with $S = 10/9$. (geometric series)

Now imagine that $\alpha \in D_d$ for some $d \geq 2$. Then there would exist an $\epsilon > 0$ such that for any fraction p/q one would have $|\zeta - p/q| > \frac{\epsilon}{q^d}$. In particular, one would have $|\zeta \frac{p_k}{q_k}| > \frac{\epsilon}{q_k^d}$. Therefore one would have

$$\frac{\epsilon}{q_k^d} < \frac{S}{q_k^{k+1}}$$

for any k. Now for k really large, this is impossible (the sequence $10^{k!(k+1-d)}$ is unbounded and therefore is not bounded by S/ϵ).

Problem 4. *Find two rational numbers a/b such that*

$$|\sqrt{2} - \frac{a}{b}| < \frac{1}{\sqrt{5}b^2}.$$

Answer. We use approximations coming from the continued fractions. The first one is $1/1$. It is easy to check that $|\sqrt{2} - 1| < 1/\sqrt{5}$. Let's try the next approximant $1 + (1/2) = 1.5$. Do we have $|\sqrt{2} - 1.5| < (1/sqrt5).\frac{1}{2^2}$?The answer is yes (check it with a calculator and then prove it by hand)