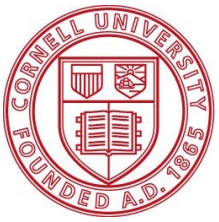

Homework # 9 Math 3340 Spring 2021

Last homework set! Due at the end of the day Wednesday, May 12.

Please submit your completed homework via gradescope on canvas. I encourage you to work with your classmates on this homework (except for the journal entries!) When you submit your work, please **list your collaborators**. (Your grade will not be affected.) Even if you work in a group, you should write up your solutions **yourself**! You should include all computational details, and proofs should be carefully written with full details. As always, please write **neatly and legibly** (feel free to use LaTeX to write up your solutions, if you wish!).

Journal entry. Let me know what you think of the material in this course (only a paragraph needed!). Some possible things to address: what was your favorite topic? What did we not cover that you would have liked to see? What should we have spent more time on? What should we have spent less time on? Did you like the textbook?

Exercises.

1. Let m and n be positive integers.

   (a) Prove that $x^m - 1$ is a factor of $x^n - 1$ in $\mathbb{Q}[x]$ if and only if $m|n$ (note: an element w in $\mathbb{C}$ such that $w^n = 1$, but no smaller power equals 1, is called a primitive n-th root of unity.)

   (b) Find the irreducible factors of $x^{12} - 1$ (over $\mathbb{Q}[x]$).

   (c) For a given n, let $g(x) = \text{lcm}\{x^d - 1 : d|n, d < n\}$. Let $f_n(x)$ be $(x^n - 1)/g(x)$. For example, $f_4(x) = x^2 + 1$. Find $f_n(x)$ for $n = 6, 9, 12$.

   Challenge (not for HW): is $f_n(x)$ irreducible over $\mathbb{Q}$, for all n?

2. A commutative ring R which has exactly one maximal ideal is called a **local ring**. Fix a prime number p. Let

$$R = \{\frac{a}{b} \in \mathbb{Q} \mid p \not| \ b\}$$

   (a) Show that R is a local ring, and find its maximal ideal.

   (b) What are the ideals of R?

   (c) Is R a field? A domain? A principal ideal domain? (Give reasons!)

3. Let R be a commutative ring. A **derivation** on R is a function $\partial : R \to R$, that satisfies the following conditions: (1) $\partial(f+g) = \partial(f) + \partial(g)$, for all $f, g \in R$, and (2) $\partial(fg) = f\partial(g) + \partial(f)g$.

   (a) Suppose that S is a commutative ring. Show that for $R = S[x]$, there is a derivation on R which satisfies $\partial(a) = 0$ for $a \in S$, and $\partial(x) = 1$. This is called **differentiation**, but note that there are no calculus limits, and in fact, S can even be a finite field.

(b) For $F = \mathbb{Z}_p$, and $R = F[x]$, let ∂ be this derivation. What is the set G of elements $f \in R$ such that $\partial(f) = 0$? Is this subset an ideal? A ring? A field?

4. Given a field F and a monic polynomial f of degree n, an extension field E of F is called a **splitting field** of f if (1) In $E[x]$, $f(x)$ factors into linear monic polynomials $x - u_i$, for $1 \leq i \leq n$, for $u_i \in E$, and (2) $E = F(u_1, \ldots, u_n)$ is the field generated by the u_i over F.

   (a) Show that if F is a field, there exists a field E containing F (rather, a field isomorphic to F) which is a splitting field of $f(x)$.

   (b) Find the splitting field (as a subfield of $\mathbb{C}$) of the polynomial $x^6 - 1 \in \mathbb{Q}[x]$.

   It is true that the splitting field of F is unique, up to isomorphism of fields (proved in the book, theorem 6.4.5, alas, we didn't have time to prove that). You may use this fact in the next problem.

5. In this problem, we examine the structure of finite fields. You may use the following result without proof: If G is a finite Abelian group, and $a \in G$ is an element of maximal order in G, then the order of every element in G is a divisor of the order of a.

   Let F be a finite field, of characteristic $p > 0$. You may use the fact that we will do in class that F has p^n elements, for some integer $n \geq 1$.

   (a) Show that there is a unique subfield of F that is isomorphic to Z_p.

   (b) Show that the group of units of F, $F^\times$, is a cyclic group.

   (c) Show that every element of F is a root of $f(x) = x^{p^n} - x$.

   (d) Show that there exists a (monic) irreducible polynomial $p(x) \in \mathbb{Z}_p[x]$ of degree n such that F is isomorphic to $\mathbb{Z}_p[x]/\langle p(x) \rangle$.

   (e) Show that F is a (and therefore, the) splitting field of $f(x)$.

   (f) Show that if F, E are finite fields with the same number of elements, then E and F are isomorphic as fields. i.e. there is really only one field of order p^n, often called $GF(p^n)$ (GF stands for "Galois field").

   (g) Find a construction of $GF(16)$.

6. In this problem you will construct a regular pentagon by compass and straightedge.

   (a) Let $\alpha = \cos(2\pi/5) + i\sin(2\pi/5) = e^{2i\pi/5}$. Show that $\alpha^5 = 1$ is a 5-th root of 1, and in fact it is a root of $(x^5 - 1)/(x - 1)$, since $\alpha \neq 1$. (You may use Euler's formula: $e^{i\theta} = \cos(\theta) + i\sin(\theta)$).

   (b) Consider $c = \alpha + \alpha^{-1}$. Use (a) to find a quadratic polynomial with root c, and use the quadratic formula to find c.

   (c) Show that $\cos(2\pi/5) = \frac{-1+\sqrt{5}}{4}$, and that $\sin(2\pi/5) = \frac{\sqrt{10+2\sqrt{5}}}{4}$.

   (d) Conclude that we can construct a regular pentagon.

   Challenge, not for HW: How do you do the actual construction? Try doing it on paper with a ruler (straightedge, but you don't get to use the markings!) and a compass.

7. Show that it is impossible to construct a regular heptagon (7 sides, all the same length) by compass and straightedge. (Hint: consider index of fields).

8. **(RSA encryption)** Bob chooses two prime numbers p, and q, that he keeps secret. Generally these have hundreds of digits, but they can be any two primes, e.g. $p = 23$, $q = 37$. Let $n = pq$. RSA encryption is based on the unproved but empirical fact that factoring the number n is not possible in polynomial time. So Bob knows p, q, but no one else can deduce these. At least that is the plan!

   A message is broken up into parts each of less than the number of digits of n. For example "hi there" might be encoded as the number $u_1 = 0809002008051805$, if this is less than m (using 01 for a, 02 for b, etc, and 00 for space). If not, it is divided up into smaller values, e.g. $u_1 = 08090020$ and $u_2 = 08051805$.

   The goal: Alice wants to send Bob a message, that no one else can read. She translates the message she wants to send into a sequence of numbers less than n, e.g. $u_1, u_2, \ldots, u_N$, where each u_i is between 0 and $n-1$. The idea is to (further) encode these numbers so that Bob can decode them, but no one else can.

   So, before hand, Bob does the following: Let e be a number such as $2^{16} + 1$ (we make sure that e is relatively prime with $p-1$ and $q-1$). Bob computes a number d from p and q such that $de \equiv 1 (\mathrm{mod} \phi(n) = (p-1)(q-1))$. Bob throws away p, q, publishes the pair of numbers (e, n) as the "public key", but keeps d secret. Even Alice doesn't know d.

   In this problem, we figure out how to encode u_i so that Bob can figure out the message, but that if someone else can figure it out, then they can factor n, which should mean that the message is safe.

   (a) Alice does the following to encode a message. For each word u_i (where $0 \leq u_i < n$), she computes $v_i := u_i^e (\mathrm{mod} n)$ (this is an easy computation, at least by computer, even for numbers with hundreds of digits). She then sends $v_1, v_2, \ldots v_N$ to Bob. Bob receives each codeword v_i. Show that Bob can recover u_i by computing $w_i = v_i^d (\mathrm{mod} n)$, that is, show that $w_i = u_i$.

   (b) Use $n = 11 \cdot 13$, choose an appropriate $e \geq 3$, and find d. What is the public key? What is the private key? Suppose the message is encoded as $w_1 = 42$ (the message is, say, "42", the answer to the universe). Find the values that Alice will send to Bob.

   (c) Suppose that $pq = M$, and $p + q = N$. Find p and q in terms of M, N. Use your method on $n = pq = 11021$, where $p + q = 210$.

   (d) In this part, we see that Eve cannot easily obtain in a mathematical manner the number d. Of course, Eve could use non mathematical methods, such as kidnapping, or power usage statistics of the decoding of elements... Basically, in this problem, we see (up to a bit of number theory) that knowing d is essentially the same as factoring $n = pq$, which is supposed to take a tremendous amount of time, and so finding d will also take a tremendous amount of time!).

   Given d, and using an algorithm based on a small amount of number theory, one can compute $\phi(n) = (p-1)(q-1)$.

   Show that given n, d, e, and $\phi(n) = (p-1)(q-1) = n - p - q + 1$, one can recover the factorization $n = pq$.

(e) Suppose that Alice and Bob have created their own RSA keys: Alice has public key (e_A, n_A) and private key d_A, while Bob's keys are (e_B, n_B) and d_B. Explain how Alice can send Bob a message that only Bob can read, yet that Bob can be sure that Alice was the one who sent it to her. (You may assume that $n_A < n_B$).