MA 294: Applied Abstract Algebra / Spring 2022
Homework assignment #11
Due at the latest ~~in class~~ by 4pm on Wednesday 5/4/2022

Problem (8) and the long prompt before it added 27 April 2022. Font is still black.

Read sections 22.5, 22.6, 22.7, 22.8, 23.1, 23.3, 23.4.

(1) Exercise 22.5.2.

(2) Exercise 22.6.1

(3) Exercise 22.8.1

(4) Find all the irreducible polynomials of degree 2, 3, and 4 in $\mathbb{Z}_2[x]$. Explain your work.

(5) Exercise 23.1.1

(6) Exercise 23.3.3. (Do not use Theorem 23.4 for the second part of the question.)

(7) Consider the ring $B = (\mathbb{Z}_2[x])_{x^4+x^3+1}$, the set of equivalence classes of polynomials in $\mathbb{Z}_2[x]$ under the congruence-modulo-$(x^4 + x^3 + 1)$ relation.

   (a) How many elements does B have?

   (b) Show that B is a field.

   (c) Find the multiplicative inverses of x and $x^2 + x + 1$ in B.

   (d) Find a generator of the multiplicative group of B.

   (e) Find an element in B of multiplicative order 5.

Send your answers to problem (8) below in the body of an email (no attachments; separate email from any other topic, please) to `medved@bu.edu` with subject "RSA".

For this problem we'll use a three-digit text-to-ascii encoding, so "A" corresponds to `065`, "B" to `066`, ..., "Z" to `090`. For example "FACE" corresponds to `070065067069`. There are websites that will do text-ascii conversion for you easily. Here's one:

`http://www.unit-conversion.info/texttools/ascii/`.

Note that you might have to take a bit of care with leading zeros if you're converting a number whose digit length is not divisible by 3. (Tip: If you're converting a number to text and getting nonsense, try adding a leading zero or two.)

To assist in computations, you may use whatever computer math package you like. If you want to run a computation online in Sage (the package used in class in Wednesday), you can do this quickly and easily at

`https://sagecell.sagemath.org/`.

In particular, you do not need to create a worksheet in CoCalc as an anonymous user — it thankfully turns out to be much easier than I suggested in class!

Sample Sage code snippet similar to Wednesday's class.

(8) (a) **You're Alice!** Bob has posted the following public key:

$(n = 5180576247533436848725507285741896875666646712250184656738435 3,\ e = 5)$.

Use Bob's public key to encode your favorite food/favorite article of clothing/favorite Wordle word/favorite (or most hated) English word. Your word should be at least 5 letters long.

(b) **You're Bob!** You created a public key using the following primes:

$p = 4987298092803879847109384798 7988103$

$q = 7091834709809809898009809809380999909851$.

Your encoding power e is the smallest integer greater than 1 that is relatively prime to $m = \varphi(pq)$.

(i) What is your public key?

(ii) What is your decoding power d?

(iii) You received the following encoded message answering the question "What's purple and commutes?"

784099679888221789206144950064098370460724879012504496733051419396295678 11

Decode this message! Be precise — don't leave off any characters.

(c) **You're Eve!** Bob posts the following public key:

$(n = 1819813065706321445503461826962733682979982619288284257509025863 27,\ e = 101)$

Alice wants to send Bob a message about her favorite song. It's a little long, so she breaks her message in half, encodes each half using Bob's public key, and sends them to Bob. But you, evil eavesdropper Eve, manage to intercept both parts! Here they are:

38628799480827012120981716017819817381150289899757166097027923389

14133972336889653592272114649465558646339379142271294786142501473 0

Break the code and decode Alice's message. What is her favorite song? Explain your work.

Additional optional exercises and reading.

(9) Let $B := \mathbb{Z}_3[x]_{x^2+x+2}$.

(a) Show that B is a field with 9 elements.

(b) Find a root α of the polynomial $y^2 + 1$ in B.

(c) Section 23.1 describes $C = \mathbb{Z}_3[x]_{x^2+1}$, another field with 9 elements. Show that the map $\psi : C \to B$ sending $f(x)$ to $f(\alpha)$ is well defined, bijective, and preserves both addition and multiplication — in other words, B and C are isomorphic as fields.

(10) Let A be a finite abelian group, and let M be the maximal order of any element of A. Prove that every $a \in A$ satisfies $a^M = 1$.

Suggested plan of action: for any elements $a, b \in A$, use (8a) on HW #6 to prove that there exists an element $c \in A$ so that $\mathrm{ord}(c) = \mathrm{lcm}(\mathrm{ord}(a), \mathrm{ord}(b))$.
Why is this enough?

- **Every finite field has p^n elements for a prime p and $n \geq 1$.** See section 23.2. The argument may be summarized as follows using the language of linear algebra: if F is a finite field, then the additive group generated by 1 must have prime order p, so that $\mathbb{Z}_p \subseteq F$. Moreover, F is a vector space of some finite dimension n over the field $\mathbb{Z}_p$ (Theorem 23.2), so that $|F| = p^n$.

- **Every finite field is isomorphic to $(\mathbb{Z}_p[x])_{\pi(x)}$ for some prime p and some irreducible $\pi(x)$ in $\mathbb{Z}_p[x]$.** Let F be a finite field; let p be the characteristic of F, and let n be the dimension of F as a vector space over $\mathbb{Z}_p$, as in section 23.2. Use the primitive element theorem to find a generator α of the multiplicative group of F. By linear algebra, the elements $1, \alpha, \alpha^2, \cdots, \alpha^n$ are linearly dependent over $\mathbb{Z}_p$. The relation they satisfy gives a polynomial $\pi(x)$ in $\mathbb{Z}_p[x]$ satisfied by α; one can show that this $\pi(x)$ is irreducible of degree n.

- **There is a finite field of order p^n for every prime p and every $n \geq 1$.** See section 23.9 for the proof that $\mathbb{Z}_p[x]$ has an irreducible polynomial of every degree n.

- **Any two finite fields of the same size are isomorphic:** See (9) above for a hint of how to prove this.

- **Proof of the primitive element theorem:** Section 20.9 proves Theorem 20.9, a characterization of cyclic groups that is used in the textbook's proof of the primitive element theorem (Theorem 23.4). In class we give a different proof of Theorem 23.4 using a lemma about orders of elements in abelian groups, in (10) above. Both arguments use the fact that a polynomial over a field of degree n has no more than n distinct roots (Theorem 22.8.2) in a key way.