Math 312/ AMS 351 (Fall '17)

Sample Questions for Final

1. Solve the system of equations

$$\begin{aligned} 2x &\equiv 1 \mod 3 \\ x &\equiv 2 \mod 7 \\ x &\equiv 7 \mod 8 \end{aligned}$$

First note that the inverse of 2 is 2 mod 3. Thus, the first equation becomes (multiply both sides be $2^{-1} = 2$)

$$x \equiv 2 \mod 3$$

We also have $x \equiv 2 \mod 7$. Thus, obviously $x \equiv 2 \mod 21$ is a solution for the first two equations. We are now reduced to

$$\begin{aligned} x &\equiv 2 \mod 21 \\ x &\equiv 7 \mod 8 \end{aligned}$$

We need to write $1 = gcd(21, 8)$ as linear combination of 21 and 8. Apply the Euclid algorithm and get

$$\begin{aligned} 21 &= 2 \cdot 8 + 5 \\ 8 &= 5 + 3 \\ 5 &= 3 + 2 \\ 3 &= 2 + 1 \end{aligned}$$

Going in reverse, we get

$$\begin{aligned} 1 &= 3 - 2 \\ &= 3 - (5 - 3) = 2 \cdot 3 - 5 \\ &= 2 \cdot (8 - 5) - 5 = 2 \cdot 8 - 3 \cdot 5 \\ &= 2 \cdot 8 - 3(21 - 2 \cdot 8) \\ &= 8 \cdot 8 - 3 \cdot 21 \end{aligned}$$

Indeed, $1 = 8 \cdot 8 - 3 \cdot 21 (= 64 - 63)$. Thus, the solution to the equation is

$$x = 2 \cdot 8 \cdot 8 - 7 \cdot 3 \cdot 21 \mod 168 (= 8 \cdot 21)$$

Get $x = -313 = 23 \mod 168$. (indeed $23 \equiv 2 \mod 21$, $23 \equiv 7 \mod 8$).

2. Can we write 12 as a linear combination of 24 and 114. If yes, find a and b such that $12 = 24a + 114b$.

   Answer: A necessary and sufficient condition to write $x = a \cdot n + b \cdot m$ is $gcd(n, m)|x$. Here, $gcd(24, 114) = 6$, and $6|12$. Thus, we can write 12 as a linear combination. By Euclid, or just by inspection, we get

$$6 = 5 \cdot 24 - 114$$

   Multiply this by 2 and get

$$12 = 10 \cdot 24 - 2 \cdot 114$$

3.
   - Compute $6^{76} \mod 13$

     By Euler, we know $6^{12} \equiv 1 \mod 13$. Thus $6^{76} = 6^{72+4} = 6^4 \mod 13$. Then $6^2 = 36 = 10 \mod 13$. Then $6^4 = (6^2)^2 = 100 = 9 \mod 13$.
   - Suppose $a \equiv 4 \mod 10$. What are the possible last 2 digits of a^n.

     We have $a \equiv 0 \mod 2$ (i.e. a is even). Thus $a^n \equiv 0 \mod 4$ for $n \geq 2$.

     On the other hand $a \equiv 4 \mod 5$. This gives a can be $5k + 4$ mod 24, i.e. 4, 9, 14, 19, or 24.

$$a \in \{4, 9, 14, 19, 24\} \mod 25$$

     For concreteness, let's take $n = 102$. We know $a^n \equiv 0 \mod 4$, we need to compute $a^{102} \mod 25$. Since, we know by Euler $a^{\phi(25)} = a^{20} = 1$. We get

$$a^{102} = a^2 \in \{4^2, 9^2, 14^2, 19^2, 24^2\} \mod 25$$

     which gives

$$a^{102} = \{16, 6, 21, 11, 1\} \mod 25$$

And $a^{102} = 0 \mod 4$

Now we need to apply the Chinese reminder theorem. Note first

$$1 = 25 - 6 \cdot 4$$

So, the answer is if $a^{102} = 16$, then

$$a^{102} = 0 \cdot 25 - 16 \cdot 6 \cdot 4 = 16 \mod 100$$

Similarly, $a^{102} \cong 6 \mod 25$ gives $a^{102} = -6 \cdot 6 \cdot 4 = 56 \mod 100$. The other 3 cases are similar.

In conclusion, starting with $a \equiv 4 \mod 10$, we get that the last 2 digits of a^{102} are: $16, 56, 96, 36, 76$ (depending on $a \mod 25$).

4. We define the quaternion group Q to be the group with 8 elements $\{\pm 1, \pm i, \pm j, \pm k\}$ such that $i^2 = j^2 = k^2 = -1$, and $ij = k$, $jk = i$, and $ki = j$. Show that Q is not isomorphic to

   - $\mathbb{Z}_8$
   - $\mathbb{Z}_4 \times \mathbb{Z}_2$
   - Σ_4
   - $D(4)$

   Q is not abelian, while $\mathbb{Z}_8$ and $\mathbb{Z}_4 \times \mathbb{Z}_2$ are abelian. Thus, they cannot be isomorphic. Q has order 8, while Σ_4 has order 24, again non-isomorphic. Finally, to distinguish Q and $D(4)$ we need to count the elements of order 4: there are 6 such elements in Q ($\pm i$, $\pm j$, $\pm k$), while there are only 2 in $D(4)$ (ρ and ρ^3, where ρ is a rotation of order 4).

5. Give an example of

   - a field with finitely many elements: $\mathbb{Z}_p$ (p prime)
   - two different examples of integral domains, which are not fields: $\mathbb{Z}$, $\mathbb{Z}_2[X]$.
   - a ring (commutative and with unit) which is not an integral domain: $\mathbb{Z}_n$
   - a ring which doesn't have a unit: $2\mathbb{Z}$

- a ring which is not commutative: $M_{n,n}(\mathbb{R})$ ($n \times n$ matrices, with real coefficients)

6. Find the decomposition into irreducible factors for

   i) $x^3 - 3x^2 + 3x - 2$ over $\mathbb{Z}_7$ Let $f = x^3 - 3x^2 + 3x - 2$. We compute $f(0) = -2$, $f(1) = -1$, $f(2) = 8 - 12 + 6 - 2 = 0$, $f(3) = 27 - 27 + 9 - 2 = 7 = 0$, $f(4) = 64 - 48 + 12 - 2 = 26$, $f(5) = 125 - 75 + 15 - 2 = 63 = 0$. Thus, we get 3 roots, 2,3, 5. We conclude
   $$f = (x-2)(x-3)(x-5)$$

   ii) $x^4 - x^2 - 6$ over $\mathbb{R}$
   $$x^4 - x^2 - 6 = (x^2 - 3)(x^2 + 2) = (x - \sqrt{3})(x + \sqrt{3})(x^2 + 2)$$

   iii) same as (ii), but over $\mathbb{C}$
   $$x^4 - x^2 - 6 = (x-\sqrt{3})(x+\sqrt{3})(x^2+2) = (x-\sqrt{3})(x+\sqrt{3})(x+i\sqrt{2})(x-i\sqrt{2})$$

7. Find the gcd and lcm of the following polynomials x^4+x+1 and x^3+x+1 over $\mathbb{Z}_3$. Use both methods: factorization and Euclid's Algorithm.

   Euclid Algorithm:

   (Step 1) divide $x^4 + x + 1$ by $x^3 + x + 1$. We get
   $$x^4 + x + 1 = x \cdot (x^3 + x + 1) + 2x^2 + 1$$

   (Step 2) divide $(x^3 + x + 1)$ by the reminder $2x^2 + 1$
   $$x^3 + x + 1 = 2x \cdot (2x^2 + 1) - (x - 1)$$

   (Step 3) Repeat: divide $2x^2 + 1$ by $x - 1$. We get
   $$(2x^2 + 1) = 2(x-1)(x+1)$$

   thus remainder 0. Euclid tells us that the last non-zero remainder (i.e. $(x - 1)$ is the gcd).

In general, we have

$$gcd(f,g) \cdot lcm(f,g) = f \cdot g$$

Thus

$$lcm = \frac{(x^4+x+1)(x^3+x+1)}{x-1} = (x^4+x+1)(x^2+x+2)$$

8. Find all irreducible cubic polynomials over $\mathbb{Z}_2$.

   List all polynomials of degree 3 over $\mathbb{Z}_2$, then eliminate those that have 0 or 1 as root. Note that 0 is a root iff the coefficient of the constant is 0, and 1 is a root iff the sum of the coefficients is even.

   Thus, we get two possibilities: x^3+x^2+1 and x^3+x+1 (the coefficient of x^3 and of the constant have to be 1, and then we need an odd number of non-zero coefficients).

9. Let $f = x^2+x+2$ over $\mathbb{Z}_3$

   i) Show that f is irreducible.
   $f(0) = 2$, $f(1) = 4 = 1$, $f(2) = 2$. Thus, degree 2 and no root; it implies irreducible.

   ii) Write down the 9 representatives for the congruence classes mod f.
   Just the polynomials of degree less than 1. Thus, answer: x, $x+1$, $x+2$, $2x$, $2x+1$, $2x+2$, 0, 1, 2.

   iii) Compute $(x+1)^3$ mod f.
   We know $x^2+x+2 = 0$ (because we work modulo x^2+x+2). Thus

   $$x^2 = 2x+1$$

   Also note

   $$x^3 = x \cdot x^2 = 2x^2 + x = 2(2x+1) + x = 2x+2$$

   Back to the question

   $$(x+1)^3 = x^3 + 3x^2 + 3x + 1 = x^3 + 1 = 2x + 3 = 2x$$

iv) Find the inverse of $[x+1]_f$.

We look for $ax+b$ such that

$$(x+1)(ax+b)=1$$

Expanding we get

$$ax^2+(a+b)x+b=1$$

Use $x^2=2x+1$ and get

$$1=ax^2+(a+b)x+b=2ax+a+(a+b)x+b=bx+(a+b)$$

giving

$$b=0, \quad a+b=1$$

Thus, $b=0$, $a=1$. Thus the inverse of $x+1$ is just x.

Let's check:

$$x(x+1)=x^2+x=2x+1+x=3x+1=1$$

10. Give example of a field with 9 elements.

    In general, the answer to such a question (a field with p^n elements, here $p=3$, $n=2$) is to say polynomials over $\mathbb{Z}_p$ modulo an **irreducible** polynomial of degree n. In this case, you are given a degree 2 polynomial over $\mathbb{Z}_3$ in the example above... ($f=x^2+x+2$). In general, you have to find such an irreducible polynomial. Typically, you can find irreducible polynomials of type x^n+a (exception over $\mathbb{Z}_2$).