MATH 227
Recitation Hour - Tuesday March 31

Some Basic Number Theory and an application to Finite Fields

Recall some terminology and facts we had seen in MATH 127:

I) Let $m, n \in \mathbb{Z}$. We say that m <u>divides</u> n (or that <u>it is a divisor of</u> n) and we write $m \mid n$, if there is another integer q such that

$$n = q \cdot m.$$

We also say that n is a <u>multiple</u> of m.

II) Let $m, n \in \mathbb{Z}$. Clearly $1 \mid m$ and $1 \mid n$, so we can ask what other integers divide both m and n. Also it's not hard to see that any integer $\geq \max\{|m|, |n|\} + 1$ cannot divide either m or n (unless we're in the trivial case that $m = n = 0$); thus it also makes sense to look for the maximum of those integers that divide both m and n. This maximum, that is, the largest positive integer that divides both m and n is called the <u>greatest common divisor</u> of m and n and is denoted by $\boxed{\gcd(m,n)}$

III) A positive integer $m > 1$ is called <u>prime</u> if its only positive divisors are 1 and m itself.
e.g. $2, 3, 5, 7, 11, 13, \ldots$ are prime, while

4, 6, 8, 9, 10, 12 are not (and are called composite numbers).

IV) Two integers m, n are called relatively prime if $\gcd(m,n) = 1$. (we also use the term coprime)

e.g. 5 and 12 are relatively prime
4 and 9 " "
4 and 10 are not relatively prime
since $\gcd(4, 10) = 2$.

We are now going to state and prove a few very beautiful facts from Basic Number Theory: in the proofs we will be relying on the Principle of Mathematical Induction, as well as on an equivalent principle

The Well-Ordering Property of $\mathbb{N}$
which states that **every non-empty subset of $\mathbb{N}$ has a minimum element.**

Interesting Side Remark The statement that, "given any set A, we can introduce an ordering "$\leq$" on A such that $(A, \leq)$ has the above property too" is equivalent to the Axiom of Choice and to Zorn's Lemma.
We usually refer to this statement as the

Well-Ordering Theorem, and we call any "good" ordering of A a well-ordering.

However, in the case of $\mathbb{N}$ the fact that the standard ordering is a well-ordering follows from the construction of $\mathbb{N}$ and does not require the Axiom of Choice.

Important Results from Number Theory

Thm 1 (Euclidean Algorithm of Division) Let m, n be integers with $m > 0$. Then there are unique $q, r \in \mathbb{Z}$ with $0 \leq r < m$ such that

$$n = q \cdot m + r$$

(Recall that q is called the quotient produced by the division algorithm, and r is called the remainder)

Proof Consider integers of the form

$$s \cdot m \qquad s \in \mathbb{Z}$$

Then, since $m > 0$ and since $\mathbb{N}$ is not bounded above (Archimedean Property), the set

$$A_{m,n} = \{ k \in \mathbb{N} : k > n \text{ and } k = sm \text{ for some } s \in \mathbb{Z} \}$$

is a non-empty subset of $\mathbb{Z}$ that is bounded below, so it can be viewed as a subset of a copy of $\mathbb{N}$.

By the Well-Ordering Property, it has a minimum element k_0, or in other words an element of the form $s_0 \cdot m$ with $s_0 \cdot m > n$ and

$(s_0 - 1) \cdot m \leq n$. (why do we have the last inequality?)

But then if we set $q = s_0 - 1$, we will have

$$q \cdot m \leq n < (q+1) \cdot m = q \cdot m + m.$$

It follows that

$$0 \leq n - qm < m,$$

so if we set $r = n - qm$, we have what we wanted (also any number $\ell \in \mathbb{Z}$ that satisfies

$$\ell \cdot m \leq n < (\ell + 1) \cdot m$$

will also satisfy that $(\ell+1) \cdot m$ is the least element of the set $A_{m,n}$, so this will imply that $\ell = q$ as defined above, showing that q, r are completely determined by the desired properties

$$n = q \cdot m + r, \quad 0 \leq r < m).$$

Thm 2 (Bézout's Identity) Let $m, n \in \mathbb{Z}$ (with at least one of them non-zero), and set $d = \gcd(m, n)$. Then we can find $k_1, \ell_1 \in \mathbb{Z}$ such that

$$d = k_1 m + \ell_1 \cdot n.$$

(note that these k_1, ℓ_1 don't have to be unique).

We can use the Euclidean Algorithm of Division to give a constructive proof of Bézout's Identity.

e.g. suppose $m = 21$ and $n = 55$

Then if we try to divide 55 by 21

we get $55 = (21) \cdot 2 + (13)$

Next, if we try to divide 21 by 13
we get $21 = 13 \cdot 1 + 8$
if we try to divide 13 by 8
we get $13 = 8 \cdot 1 + 5$
if we try to divide 8 by 5
we get $8 = 5 \cdot 1 + 3$
if we try to divide 5 by 3
we get $5 = 3 \cdot 1 + 2$
if we try to divide 3 by 2
we get $3 = 2 \cdot 1 + 1$
if we try to divide 2 by 1
we get $2 = 1 \cdot 2 + 0$

This also shows that $1 = \gcd(55, 21)$.
We now reverse the process:

$$1 = 3 - 1 \cdot 2 = 3 - (5 - 1 \cdot 3) = 2 \cdot 3 - 5$$
$$= 2 \cdot (8 - 1 \cdot 5) - 5 = 8 - 3 \cdot 5 = 8 - 3 \cdot (13 - 1 \cdot 8)$$
$$= 4 \cdot 8 - 3 \cdot 13 = 4 \cdot (21 - 1 \cdot 13) - 3 \cdot 13 = 4 \cdot 21 - 7 \cdot 13$$
$$= 4 \cdot 21 - 7 \cdot (55 - 2 \cdot 21) = 18 \cdot 21 - 7 \cdot 55.$$

Alternative proof of Bézout's identity:
We will need the following notion from Algebra (and in particular Ring Theory):
Definition Let R be a commutative ring.
A subset I of R is called an ideal of R if

- it is nonempty
- it is closed under addition and under taking additive inverses
- for every $x \in \mathcal{I}$ and every $r \in R$ we have $r \cdot x \in \mathcal{I}$

{ note that this property is stronger than saying that $\mathcal{I}$ is closed under multiplication (why?)

Some examples of ideals:

1) $R = \mathbb{Z}$, $\mathcal{I}_1 = 2\mathbb{Z} = \{\text{even integers}\}$
$\mathcal{I}_1 = 5\mathbb{Z} = \{\text{multiples of } 5\}$

2) $R = \mathbb{Q}^3$ viewed as a ring with componentwise addition and multiplication,
$\mathcal{I} = \left\{ \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \in \mathbb{Q}^3 : x_3 = 0 \right\}$

Example related to the proof of Bézout's identity:
consider the set

$$C = \{ x \in \mathbb{Z} : \exists\, k, \ell \in \mathbb{Z} \text{ such that } x = k \cdot m + \ell \cdot n \}$$

(that is, C contains all integers of the form that we want to show $d = \gcd(m,n)$ also has).

Then C is an ideal of $\mathbb{Z}$.
Indeed, C contains all multiples of m (since we can write such multiples as $k \cdot m = k \cdot m + 0 \cdot n$ for $k \in \mathbb{Z}$). Similarly, it contains all multiples of n. Thus C is nonempty.

Moreover if $x_1, x_2 \in C$, then we can find integers k_1, k_2, l_1, l_2 such that

$$x_1 = k_1 \cdot m + l_1 \cdot n, \quad x_2 = k_2 \cdot m + l_2 \cdot n.$$

But then

$$x_1 + x_2 = (k_1 + k_2) \cdot m + (l_1 + l_2) \cdot n \in C$$

and $$-x_1 = (-k_1) \cdot m + (-l_1) \cdot n \in C.$$

Finally, for any $r \in \mathbb{Z}$ we have

$$r \cdot x_1 = r \cdot (k_1 \cdot m + l_1 \cdot n) = (r \cdot k_1) \cdot m + (r \cdot l_1) \cdot n \in C.$$

Now we want to show that $d = \gcd(m,n) \in C$.
Consider the set $C \cap \mathbb{N}$. This is a nonempty subset of $\mathbb{N}$ (since C contains positive multiples of m or n as well (recall that at least one of m, n is non-zero)).
But then, by the Well-Ordering Property of $\mathbb{N}$, we know that $C \cap \mathbb{N}$ has a minimum element e.

We will show that $d = e \in C$.

<u>Step 1</u> Show that $d \leq e$.

We know that $e \in C$, so there are integers k_0, l_0 such that $e = k_0 \cdot m + l_0 \cdot n$.
But then, since $d \mid m$ and $d \mid n$, we have that $d \mid e$ as well. Given that both d and e are positive integers, we can conclude that $d \leq e$.

Step 2 show that $e \leq d$.

Recall that d here stands for the greatest common divisor of m and n. Thus if we manage to show that e is a common divisor of m and n too, we will be done, because we will necessarily have that $e \leq \gcd(m,n) = d$.

Assume towards a contradiction that e does not divide m. Then by the Euclidean Algorithm of Division we can write

$$m = q_1 \cdot e + r_1 \quad \text{for some } q_1, r_1 \in \mathbb{Z}$$

and with r_1 satisfying $\boxed{0 < r_1 < e}$

But then, since C is an ideal of $\mathbb{Z}$, and since $m, e \in C$, we obtain that

$$m, q_1 \cdot e \in C \Rightarrow r_1 = m - q_1 \cdot e \in C.$$

Thus $r_1 \in C \cap \mathbb{N}$ and $r_1 < e$, which is a contradiction with what we set e to be: the minimum element of $C \cap \mathbb{N}$.

Thus the assumption that e does not divide m was incorrect, and we can conclude that $e \mid m$.

Similarly, we verify that $e \mid n$.

As said above, these combined give that $e \leq d$.

We can finally conclude that $d = e = \min(C \cap \mathbb{N}) \in C$.