417 lecture 3 Integer Arithmetic.

Integer arithmetic will be important in this course:
- It provides examples of abstract concepts.
- We will use integer arithmetic even when studying completely abstract groups.

Most of this is stuff you already know, but the presentation may be more formal now.

Natural numbers $\mathbb{N} = \{1, 2, 3, \dots\}$
Integers $\mathbb{Z} = \{0, \pm 1, \pm 2, \cdots\}$

$\mathbb{N}$ is the same as the set of <u>positive integers</u>.
The set of nonnegative integers is $\{0, 1, 2, ..\} = \mathbb{N} \cup \{0\}$

We write $a > 0 \iff a \in \mathbb{N}$
$a \geq 0 \iff a \in \mathbb{N} \cup \{0\}$

$$|a| = \begin{cases} a & \text{if } a \geq 0, \\ -a & \text{otherwise} \end{cases}$$ thus $|a| \geq 0$ always

There are operations $+$ and $\cdot$ and for all $a, b, c \in \mathbb{Z}$,

(1) $a + b = b + a$, $(a+b)+c = a + (b+c)$
$+$ is commutative and associative

(2) $ab = ba$, $(ab)c = a(bc)$
$\cdot$ is commutative and associative

(3) $0 + a = a$
0 is the identity element for $+$

(4) $1 \cdot a = a$
1 is the identity element for $\cdot$

(5) for any a, there is an element $-a$ such that $a + (-a) = 0$. We write $b - a$ for $b + (-a)$
(additive inverses exist)

We write $b > a$ if $b - a > 0$, ie. $b - a \in \mathbb{N}$

(6) $a(b+c) = ab + ac$
Distributive law

(7) If $a, b > 0$ then $a + b > 0$ and $ab > 0$
($\mathbb{N}$ is closed under addition and multiplication)

(8) If $a \neq 0$ and $b \neq 0$ then $ab \neq 0$.

In fact $|ab| \geq \max\{|a|, |b|\}$.

We shall take all of the above properties as known.

<u>Divisibility</u>:

<u>Definition</u> Let $a, b \in \mathbb{Z}$. We say <u>a divides b</u>, $a \mid b$ if there is a $q \in \mathbb{Z}$ such that

$$b = aq.$$

"a divides b" $\Leftrightarrow$ "b is divisible by a" $\Leftrightarrow$ "b is a multiple of a"
$\Leftrightarrow$ "a is a divisor of b"

<u>Proposition</u>: Let a, b, c, u, v be integers.

(a) if $uv = 1$, then $u = v = 1$ or $u = v = -1$.
(b) If $a|b$ and $b|a$ then $a = b$ or $a = -b$.
(c) If $a|b$ and $b|c$ then $a|c$
(d) If $a|b$ and $a|c$ then $a|(ub+vc)$.

<u>Proofs</u> of (c), (d) – see Goodman for others.

(c) Suppose $a|b$ and $b|c$. Then there are $q_1, q_2 \in \mathbb{Z}$ such that $b = q_1 a$ and $c = q_2 b$

then $c = q_2 b = q_2(q_1 a) = (q_2 q_1) a$
which shows $a|c$

(d) suppose $a|b$ and $a|c$ then there are $q, r \in \mathbb{Z}$ such that $b = qa$ and $c = ra$
then

$$ub + vc = u(qa) + v(ra) = (uq)a + (vr)a = (uq+vr)a$$

thus $a | ub+vc$. ▨

<u>Definition</u> A natural number $p \in \mathbb{N}$ is <u>prime</u> if $p > 1$ and the only $a \in \mathbb{N}$ such that $a|p$ are $a = 1$ and $a = p$

<u>Proposition</u>: Any natural number $n > 1$ is a product of prime numbers.

Proof This proof uses "strong induction".

Base case: $n=2$. Since 2 is prime, it is a product of primes with just one factor.

Induction step: Hypothesis: every r with $2 \leq r < n$ is a product of primes. We claim it follows that n is a product of primes.

Case: if n is prime, then $n=n$ is product of primes with one factor.

Case: if n is not prime, we can write $n=ab$ with $a>1, b>1$. then $2 \leq a < n$ and $2 \leq b < n$ so they are products of primes by hypothesis.

$$a = p_1 p_2 \cdots p_s \qquad b = p_1' \, p_2' \cdots p_r'$$

so $n = ab = p_1 p_2 \cdots p_s p_1' p_2' \cdots p_r'$ is a product of primes $\square$

Note: It is useful to think that 1 is a product of primes as well: It is the "empty product", with zero factors. This is a sort of "edge case".

List of primes $2, 3, 5, 7, 11, 13, 17, \ldots$

Proposition: There are infinitely many primes.

Proof: Suppose there are finitely many primes; list them as $p_1, p_2, \ldots, p_r$.

Set $N = p_1 p_2 \cdots p_r + 1$. By previous proposition,

N is a product of primes, so some p_i divides N, and we may write $p_i \mid N$.
On the other hand $p_i \mid p_1 \cdots p_r$ obviously, so $p_i \mid N-1$.

Since $p \mid N$ and $p \mid N-1$, p divides $N-(N-1) = 1$
$p \mid 1$ means $1 = pq$, but this implies $p = q = \pm 1$, which is absurd since $p > 1$. $\blacksquare$

Back to elementary school:

<u>Proposition</u> (integer division with remainder)
Given $a, d \in \mathbb{Z}$ with $d > 1$, there are unique $q, r \in \mathbb{Z}$ such that $a = qd + r$ and $0 \le r < d$.
q = "quotient"
r = "remainder"

<u>Example</u>:

$$\begin{array}{r} 54 \\ 7 \overline{\smash{)}381} \\ -35 \\ \hline 31 \\ -28 \\ \hline 3 \end{array}$$

$q = 54$ $r = 3$

$381 = 54 \cdot 7 + 3$ true
$0 \le 3 < 7$ true

<u>Proof</u>: Case $a \geq 0$. If $a < d$, then $q = 0$ $r = a$ works since $a = 0 \cdot d + a$ and $0 \le a < d$.
Use this as the base case for strong induction.
Hypothesis: for all b with $0 \le b < a$, we can find q_0, r_0 such that $b = q_0 d + r_0$ and $0 \le r_0 < d$

Since case $a < d$ was dealt with, we consider $d \le a$ then $0 \le a - d < a$ so we can find q_0, r_0 such that

$$a-d = q_0 d + r_0 \qquad 0 \le r_0 < d.$$

Then $a = q_0 d + d + r_0 = (q_0+1)d + r_0$ take $q = q_0 + 1$, $r = r_0$

For $a<0$, apply above result to $-a>0$. then

$$-a = q_0 d + r_0 \quad \text{so} \quad a = -q_0 d - r_0$$

If $r_0 = 0$, take $q = -q_0$ and $r = r_0$

If $r_0 \neq 0$, then $-d < -r_0 < 0$ so $0 < r_0 + d < d$

so write $a = (-q_0 - 1)d + (r_0 + d)$ take $q = -q_0 - 1$
$r = r_0 + d$

For uniqueness, suppose

$a = qd + r$ and $a = q'd + r'$ where $0 \le r < d$
and $0 \le r' < d$

then subtracting one from the other,

$$0 = a - a = qd + r - (q'd + r') = (q-q')d + (r-r')$$

or $r' - r = (q-q')d$, so $d \mid (r'-r)$

since $|r'-r| < d$, we must have $r'-r = 0$ so $r' = r$

then $(q-q')d = 0$ so $q = q'$ as well (as $d \neq 0$) ∎

<u>Definition</u> Let $n, m \in \mathbb{Z}$ be non zero integers.

the <u>greatest common diviser</u> of m, n is the natural number d such that

(i) $d \mid m$ and $d \mid n$ and

(ii) if $x \mid m$ and $x \mid n$, then $x \mid d$.

We write $d = \gcd(m,n)$.

m and n are called <u>relatively prime</u> if $\gcd(m,n) = 1$

There is an algorithm to compute the gcd of m and n. Apply division with remainder repeatedly, each time where the dividend and divisor are the divisor and remainder from the previous step. Stop when you get remainder 0.

<u>Example</u> $\gcd(54, 44) = 2$

$$54 = 1\cdot 44 + 10 \Longrightarrow 2 \text{ divides } 54 \text{ and } 44$$

$$\Uparrow$$

$$44 = 4\cdot 10 + 4 \Longrightarrow 2 \text{ divides } 44 \text{ and } 10$$

$$\Uparrow$$

$$10 = 2\cdot 4 + 2 \Longrightarrow 2 \text{ divides } 10 \text{ and } 4$$

$$\Uparrow$$

$$4 = 2\cdot \underset{\text{gcd}}{\boxed{2}} + 0 \Longrightarrow 2 \text{ divides } 4 \text{ and } 2$$

Moreover, we can write 2 as a combination of 54 and 44

$$\begin{aligned}
2 &= 10 - 2\cdot 4 \\
&= (54-44) - 2(44 - 4\cdot 10) \\
&= (54-44) - 2(44 - 4(54-44)) \\
&= 54 - 44 - 2\cdot 44 + 8\cdot 54 - 8\cdot 44 \\
&= 9\cdot 54 - 11\cdot 44
\end{aligned}$$

With this representation, we see that if $x \mid 54$ and $x \mid 44$, then $x \mid 9\cdot 54 - 11\cdot 44 = 2$. Thus 2 really is the gcd.

In general,

<u>Proposition</u> For any non-zero integers n and m, there are integers a and b such that $\gcd(m,n) = am + bn$.