MATH 2020 Lecture 3

Chapter 2

Recall mathematical induction: (principle of induction)

If $S(n)$ is a statement about integers that depends on the variable n, suppose that $S(n_0)$ is true for some $n_0 \in \mathbb{N}$.

If $S(K)$ true implies $S(k+1)$ is true, then $S(n)$ is true for all $n \geq n_0$.

Example: Prove that

$$10^{n+1} + 3 \cdot 10^n + 5$$

is divisible by 9 for every $n \in \mathbb{N}$.

Proof: We start with $n=1$, and find

$$10^{1+1} + 3 \cdot 10^1 + 5 = 100 + 30 + 5 = 135 = 9 \cdot 15,$$

so the statement:

$S(n): 10^{n+1} + 3 \cdot 10^n + 5$

is true for $n_0 = 1$.

Now suppose that $10^{k+1} + 3 \cdot 10^k + 5$ is divisible by 9. Then $S(k+1)$ is true, since

$$10^{(k+1)+1} + 3 \cdot 10^{k+1} + 5$$

$$= 10\left(10^{k+1} + 3 \cdot 10^k\right) + 5$$

$$= 10(10^{k+1} + 3\cdot 10^k) + 50 - 45$$

$$= \underbrace{10(10^{k+1} + 3\cdot 10^k + 5)}_{\text{divisible by 9, by assumption}} - \underbrace{45}_{\text{divisible by 9.}}$$

Therefore $S(k+1)$ is true, ie. $10^{(k+1)+1} + 3\cdot 10^{k+1} + 5$ is divisible by 9. By induction, $S(n)$ is true for all n.

There is another approach to induction:
Sometimes, after showing that $S(n_0)$ is true for a particular n_0, we will begin our proof by assuming that $S(n_0)$, $S(n_0+1)$, $S(n_0+2)$, $\cdots$, $S(n_0+k)$ are true. Then prove $S(n_0+k+1)$ is true from these assumptions. The conclusion is the same: $S(n)$ is true for all n.

Definition: A set $S \subset \mathbb{Z}$ is well-ordered if it contains a smallest element. (In general, an ordered set is well-ordered if every subset has a least element).

Principle of well-ordering: Every nonempty subset of $\mathbb{N}$ contains a smallest element.

Remark:
The well-ordering principle is equivalent to the principle of mathematical induction

§2.2 The division algorithm. (Application of well-ordering)

Theorem: Let $a, b \in \mathbb{Z}$ with $b > 0$. Then there are unique q, r such that

$$a = bq + r, \quad \text{where } 0 \le r < b.$$

Proof: We do two steps: First we show q and r exist, then show that they are unique.

Existence: Set $S = \{a - bk \mid k \in \mathbb{Z} \text{ and } a - bk \ge 0\}$.

If $0 \in S$, then $a - bk = 0$ and so taking $q = \frac{a}{b}$ and $r = 0$ works.

If $0 \notin S$, then since S is nonempty (check this!) it has a smallest element, say $r \in S$ is smallest. So $r = a - bq$ for some q, and $a = bq + r$, $r \ge 0$.

We must show $r < b$.

If $r > b$, then

$$a - b(q+1) = a - bq - b = r - b > 0$$

and so $a - b(q+1) \in S$. But also $a - b(q+1) < \underset{\overset{\parallel}{r}}{a - bq}$,

which would contradict r being the smallest.

Thus $r \leq b$. Since $0 \notin S$, $r \neq b$, so $r < b$.

Uniqueness of r and b: Assume that there are integers r', q' with $a = bq' + r'$ and $0 \leq r' < b$.

Then $bq + r = bq' + r'$. If $r' \geq r$, then

$b(q - q') = r' - r \Rightarrow b$ divides $r' - r$, and

$0 \leq r' - r \leq r' < b$. This is only possible if $r - r' = 0$,

so $r = r'$ and $q = q'$.

If $b = ak$ for some k, write $a \mid b$. If $a \mid b$ and $a \mid c$, then a is called a common divisor of b and c.

Denote the greatest common divisor of b and c by $\gcd(b, c)$. Say b and c are relatively prime if $\gcd(b, c) = 1$.

MATH 2020 Lecture 4.

§ 2.2. The division algorithm continued.

Last day we saw that for $a, b \in \mathbb{Z}$ with $b > 0$, there exists a unique q, r with

$$a = bq + r \quad , \quad 0 \leq r < b.$$

Next:

Definitions: If $b = ak$ (where $b, a, k \in \mathbb{Z}$), we write $a|b$ and say "a divides b". A *common divisor* of integers a and b is an integer d with $d|a$ and $d|b$. The *greatest common divisor* of a and b is an integer $\gcd(a,b)$ satisfying: If d is any common divisor of a and b, then $d | \gcd(a,b)$. Integers a and b are *relatively prime* if $\gcd(a,b) = 1$.

Theorem 2.4: Suppose $a, b \in \mathbb{Z}$ are nonzero. Then there exist integers r and s with $ar + bs = \gcd(a,b)$. In particular, if a and b are relatively prime then $\gcd(a,b) = 1$ so $ar + bs = 1$.

Proof: Fix integers a and b.

Let $S = \{am + bn \mid m, n \in \mathbb{Z} \text{ and } am + bn > 0\}$.

Then S is nonempty, and so has a smallest element by the well-ordering principle. Say

$d = ar + bs$ is the smallest.

We'll prove that $d = \gcd(a,b)$ by showing d is a divisor, and that any other divisor d' satisfies $d' \mid d$.

To see that d is a divisor, write

$a = dq + r'$ where $0 \leq r' < d$, this is possible by last day's theorem.

$$\Rightarrow r' = a - dq$$

$$= a - (ar+bs)q = a(1-rq) + b(-sq)$$

So $r' \in S$, if $r' > 0$. But this would contradict minimality of d, so $r = 0$, and so $a = dq$ and $d \mid a$.

By an identical argument $d \mid b$, so d is a common divisor.

Suppose d' is some other divisor. Then

$a = d'h$ and $b = d'k$, so

$$d = ar + bs = d'hr + d'ks = d'(hr+ks),$$

so $d' \mid d$.

==========|END PROOF|==========

The Euclidean Algorithm is a way to compute gcd's of a pair (a, b). Suppose $a > b$, and write

$$a = bq_1 + r_1 \qquad 0 \le r_1 < b$$

then

$$b = r_1 q_2 + r_2 \qquad 0 \le r_2 < r_1$$

$$r_1 = r_2 q_3 + r_3 \qquad 0 \le r_3 < r_2$$

$$\vdots$$

$$r_k = r_{k+1} q_{k+2} + 0$$

must get zero eventually since the r's decrease.

The last nonzero r_i is the gcd.

Example: If $a = 103$ and $b = 42$, then

$$103 = 42 \cdot 2 + 19$$

$$42 = 19 \cdot 2 + 4$$

$$19 = 4 \cdot 4 + 3$$

$$4 = 3 \cdot 1 + 1$$

$$3 = 1 \cdot 3 + 0$$

the gcd of 103 and 42 is 1.

$\Rightarrow$ 103 and 42 are relatively prime.

Going in reverse, this algorithm lets us find r, s so that $ar+bs=\gcd(a,b)$. By repeated substitutions we find:

$$\begin{aligned} 1 &= 4 - 3\cdot 1 \\ &= 4 - (19-4\cdot 4)\cdot 1 \\ &= 5\cdot 4 - 19 \\ &= 5(42-19\cdot 2) - 19 \\ &= 5(42) - 11\cdot 19 \\ &= 5\cdot 42 - 11\cdot(103-42\cdot 2) \\ &= 27\cdot 42 - 11\cdot 103. \end{aligned}$$

So $1 = 27b - 11a$.

Prime numbers:

Let $n>1$. Then n is prime if its only divisors are 1 and n, if n is not prime it's called composite.

Lemma (Euclid): Let $a, b \in \mathbb{Z}$ and p prime. If $p \mid ab$ then $p \mid a$ or $p \mid b$!

Suppose $p \mid ab$.

Proof: If $p \nmid a$, then $\gcd(p, a) = 1$. So there exist r, s with

$$ps + ar = 1.$$

So $b = b \cdot 1 = b(ar + ps) = (ab)r + p(bs)$.

(ab: divisible by p; $p(bs)$: divisible by p.)

So $p \mid b$. ∎

Theorem: There are infinitely many primes.

Proof: Suppose not, say $p_1, p_2, \ldots, p_n$ is a complete list. Set $P = p_1 p_2 \cdots p_n + 1$. Then P must be divisible by something, in particular suppose by one of the primes p_i. But then $1 = \underbrace{P - p_1 p_2 \cdots p_n}$ divisible by p_i yields a contradiction, since $p_i > 1$.

So either there's an additional prime P not in our list, or P itself is prime. In either case, our list $\{p_1, \ldots, p_n\}$ missed at least one prime.

Theorem: (Fundamental theorem of arithmetic)
Let $n > 1$ be an integer. Then

$$n = p_1 \cdots p_k$$

where $p_1, \ldots, p_k$ are all primes (not necessarily distinct) and this factorization is unique. That is, if

$$n = q_1 \cdots q_\ell$$

for some primes $q_1, \ldots, q_\ell$, then $k = \ell$ and the q_j's are just a rearrangement of the p_i's.

Proof: We will use this without proof, though the proof is available to you on page 31.

MATH 2020 Chapter 3 Lecture 5

The integers mod n

Recall that we divided $\mathbb{Z}$ into equivalence classes as follows. For a fixed $n \in \mathbb{N}$, set

$$X_i = \{m \in \mathbb{Z} \mid m = i + kn \text{ for some } k \in \mathbb{Z}\}.$$

If two integers lie in the same X_i, the are equivalent and we write "$a \equiv b \bmod n$", meaning $n \mid a-b$. Denote X_i by $[i]$ (equivalence class), and then write $\mathbb{Z}_n$ for the set of equivalence classes.

Example: If $n = 6$ then

$$\mathbb{Z}_6 = \{[0], [1], [2], [3], [4], [5]\}$$

$$= \{\{\ldots -12, -6, 0, 6, 12\}, \{\ldots -11, -5, 1, 7, 13, \ldots\},$$
$$\{\ldots -10, -4, 2, 8, 14, \ldots\}, \{\ldots, -9, -3, 3, 9, 15, \ldots\},$$
$$\{\ldots, -8, -2, 4, 10, 16, \ldots\}, \{\ldots, -7, -1, 5, 11, 17, \ldots\}\}.$$

Whenever is possible, we will write 0, 1, 2, 3, 4, 5 in place of the classes $[0], [1], [2], [3], [4], [5]$, usually writing "mod n" (or in our case "mod 6")

at the end of each line of calculations to indicate that we are speaking of equivalence classes.

We can add elements of $\mathbb{Z}_n$. Define

$$[a] + [b] = [a+b]$$

ie. $a \bmod n + b \bmod n = a+b \bmod n$, similarly multiply:

$$[a] \cdot [b] = [ab].$$

ie. $(a \bmod n)(b \bmod n) = ab \bmod n$.

For example, here is multiplication in $\mathbb{Z}_4$:

	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Examples:

$6+7 \equiv 3 \bmod 5$ $\qquad$ $18-1 \equiv 1 \bmod 4$

$10 \cdot 3 \equiv 0 \bmod 10$ $\qquad$ $4 \cdot 5 \equiv 6 \bmod 7$.

Proposition: If $\mathbb{Z}_n$ is the equivalence classes of integers mod n, and $a, b, c \in \mathbb{Z}_n$ then:

(1) Addition and multiplication as defined above are commutative:

$$a+b \equiv b+a \pmod{n}$$
$$ab \equiv ba \pmod{n}.$$

(2) Addition and multiplication are associative:

$$(a+b)+c \equiv a+(b+c) \pmod{n}$$
$$(a\cdot b)c \equiv a\cdot(b\cdot c) \pmod{n}.$$

(3) There is an additive identity and there is a multiplicative identity, in the sense that

$$a+0 \equiv a \pmod{n}$$
$$a\cdot 1 \equiv a \pmod{n}.$$

(4) Multiplication distributes over addition:

$$a(b+c) \equiv ab+ac \pmod{n}.$$

(5). For every integer there is an additive inverse:

$$a+(-a) \equiv 0 \pmod{n}$$

(6) If $a \neq 0$, then a has a multiplicative inverse mod n if and only if $\gcd(a,n)=1$.

Proof: We'll prove (1) and (6). So to prove this, recall $a \equiv b \bmod n$ if and only if $a-b$ is divisible by n.

To prove (1):

Therefore $a+b \equiv b+a \pmod{n}$ since $a+b$ and $b+a$ both have the same remainder when we divide by n.

Equivalently, since $(a+b)-(b+a) = 0$, and 0 is divisible by n, we know $a+b \equiv b+a \pmod{n}$.

Similarly $ab-ba=0$ and $n \mid 0$, so $ab \equiv ba \bmod n$.

To prove (6):

Suppose $\gcd(a,n)=1$, and choose r, s so that $ar+ns=1$. Then $ns = 1-ar$, so $ar \equiv 1 \bmod n$.

Therefore the equivalence class of r, call it b, is the multiplicative inverse of $a \bmod n$.

On the other hand, if there's a "b" so that $ab \equiv 1 \bmod n$, then $n \mid ab-1$, so there's an integer k with $ab-1 = nk$. Therefore $ab-nk=1$, so if $d=\gcd(a,n)$ then d must divide $ab-nk=1$. So $d=1$ and a, n are relatively prime.

Conclusion: The set of elements $\mathbb{Z}_n$ has an addition and multiplication on it, much like the integers do, but it is something new and different!

Suggested problems: Ch 2 1-11, 15, 16, -30