MTH4104 Cheat Sheet

Shu Sasaki

13th February 2024

1 Chapter 2 and Chapter 3 (Week 1-3)

GOAL: Get used to an axiomatic approach to mathematics– given definitions/axioms, derive general statements about integers (that we know too well) via proofs and careful inspection of definitions etc.

Proposition 1. Let a and b be integers and suppose $b > 0$. Then $a = bq + r$ for some integers q and $0 \leq r < b$. The pair (q, r) is unique.

Definition. Let a and b be integers. We say that a divides b if there exists an integer c such that $b = ac$.

Remark. The only integer 0 divides is 0 itself.

Definition. Let a and b be integers. A common divisor of a and b is a non-negative integer s such that s divides both a and b. A gcd of a and b is the common divisor r satisfying the property that if s is another (different) common divisor of a and b, then $s < r$.

Proposition 2. s divides r.

We can say something similar for the lcm of a and b.

Proposition 4. If a is a non-negative integer, $\gcd(a, 0) = a$. This is not a definition.

Lemma 5. $\gcd(a, b) = \gcd(-a, b) = \gcd(a, -b) = \gcd(-a, -b)$. This is not a definition.

Theorem 7 (Bezout's identity). Let a and b be integers. Then there exist integers r and s such that $ar + bs = \gcd(a, b)$.

The proof of Bezout explains only that these integers r and s exist and does not shed any light on how to actually find them. In practice, we make appeal to Euclid's algorithm instead.

Euclid's algorithm is based on the following proposition:

Proposition 6. Let a and b be integers. Suppose $b > 0$. By Proposition 1, there exists a uniqe pair of integers q and $0 \le r < b$ such that $a = bq + r$. Then $\gcd(a, b) = \gcd(b, r)$.

How do we use Euclid's algorithm to find r and s satisfying $ar + bs = \gcd(a, b)$?

(NON-EXAMINABLE) If your Euclid's algorithm looks like:

$$\begin{array}{rrcl} & & \vdots & \\ (s_n) & r_{n-2} & = & r_{n-1}q_n + r_n \\ (s_{n+1}) & r_{n-1} & = & r_n q_{n+1} + r_{n+1} \\ & & \vdots & \\ (s_N) & r_{N-1} & = & r_N q_{N+1} + r_{N+1} \\ (s_{N+1}) & r_N & = & r_{N+1} q_{N+2} \end{array}$$

then we know that $\gcd(a, b)$ is r_{N+1}, because we may repeat Proposition 6 to deduce that

$$\gcd(a, b) = \cdots = \gcd(r_{n-2}, r_{n-1}) \overset{(s_n)}{=} \gcd(r_{n-1}, r_n) \overset{(s_{n+1})}{=} \gcd(r_n, r_{n+1}) = \cdots = \\ \gcd(r_{N-1}, r_N) \overset{(s_N)}{=} \gcd(r_N, r_{N+1}) \overset{(s_{N+1})}{=} r_{N+1}.$$

We also see from (s_N) that $r_{N+1} = -q_{N+1} r_N + r_{N-1}$. Indeed, for every n (e.g. $N, N-1, \dots$), there exist integers X_n and Y_n satisfying

$$r_{N+1} = X_n r_n + Y_n r_{n-1}.$$

This will find us r and s such that $ar + bs = r_{N+1}$.

We may prove the assertion by induction 'in reverse' (one can reindex all to make this rigorous). We saw $(X_N, Y_N) = (-q_N, 1)$ does the job. Supposing that there exist integers X_n and Y_n such that

$$r_{N+1} = X_n r_n + Y_n r_{n-1},$$

we aim at proving that there exists X_{n-1} and Y_{n-1} such that

$$r_{N+1} = X_{n-1} r_{n-1} + Y_{n-1} r_{n-2}.$$

We will spell out X_{n-1} and Y_{n-1} in terms of X_n and Y_n. To see this, plug $r_n = (-q_n) r_{n-1} + r_{n-2}$ obtained from (s_n) into $r_{N+1} = X_n r_n + Y_n r_{n-1}$. We then get

$$r_{N+1} = X_n((-q_n) r_{n-1} + r_{n-2}) + Y_n r_{n-1} = (-q_n X_n + Y_n) r_{n-1} + X_n r_{n-2},$$

hence $(X_{n-1}, Y_{n-1}) = (-q_n X_n + Y_n, X_n)$ does the job. It is possible to use this inductively (as n decreases) to find X's and Y's, starting with $(X_N, Y_N) = (-q_N, 1)$.

Definition. A prime number is a positive integer n whose positive integer divisor is 1 or itself. Alternatively, we may define it as a positive integer whose integer divisors are $\{\pm 1, \pm n\}$.

By Bezout, this is equivalent to the following: if a and b are integers and n divides ab, then n divides either a or b. The latter definition allows us to prove:

Theorem 8 (the Fundamental Theorem of Arithmetic). Every integer is of the form

$$(-1)^{r_\infty} \prod_p p^{r_p}$$

for some non-negative integers r_∞ and r_p, up to reordering of prime factors. The power r_p is the maximum number of time p divides the integer. For example, $45 = 3^2 \cdot 5$ so $r_p = 0$ if p is not 3 nor 5, $r_3 = 2, r_5 = 1$ and $r_\infty = 0$.

Let $\mathcal{R}$ be a relation on S. We let $[a] = [a]_{\mathcal{R}}$ denote the subset of all b in S which are related to a, i.e. $a\mathcal{R}b$. If $\mathcal{R}$ is an equivalence relation (satisfying a set of conditions), then

$$a\mathcal{R}b \text{ if and only if } [a] = [b].$$

Theorem 9. Given a set S, there exists a bijective correspondence between

- the equivalence relations $\mathcal{R}$ on S,
- the partitions $\mathcal{P}$ (a set of subsets of S satisfying certain conditions) on S.

Proposition 10. Let n be a positive integer. Then $(\mathcal{R}, S) = (\equiv \mathbb{Z})$, defined such that $a \equiv b \mod n$ if and only if n divides $b - a$ (for integers a and b), is an equivalence relation.

Definition. Let $\mathbb{Z}_n$ denote the set of equivalence classes $[a]$ with respect to $(\equiv, \mathbb{Z})$.

Since $a \equiv b \mod n$ if and only if $[a] = [b]$, a lot of equivalence classes may be identified. Indeed,

Proposition 11. $|\mathbb{Z}_n| = n$.

Proposition 1 proves Proposition 11. Indeed, if a is an integer (n is, by definition, a positive integer), then there exists q and $0 \leq r < n$ such that $a = nq + r$. Therefore $a \equiv r$, i.e. $[a] = [r]$. The proof also elaborates that $\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}$. The element $[r]$ is nothing other than the set of integers b with remainder r when divided by n (i.e. $b \equiv r \mod n$).

On $\mathbb{Z}_n$, we define $+, -, \times$:

$$\begin{aligned} [a] + [b] &= [a+b] \\ [a] - [b] &= [a-b] \\ [a][b] &= [ab] \end{aligned}$$

but no division. These do not depend on choice of representatives, i.e. if $a \equiv a' \mod n$, then $[a] + [b] = [a'] + [b]$ etc.

No division is defined but:

Definition. We say that $[a]$ of $\mathbb{Z}_n$ has multiplicative inverse if there exists an integer b such that $[a][b] = [1]$ (or equivalently $ab \equiv 1 \mod n$). This plays the role of $1/[a]$ but not literally ($1/[a]$ or $[1/a]$ simply does not make sense!). The multiplicative inverse is often written as $[a]^{-1}$.

Remark. The multiplicative inverse, if exists, is unique. Suppose that $[b]$ and $[c]$ are elements of $\mathbb{Z}_n$ such that $[a][b] = [1]$ and $[a][c] = [1]$. Multiplying both sides of $[c][a] = [1]$ by $[b]$, we obtain $[c][a][b] = [1][b]$, i.e. $[c] = [b]$.

Theorem 12. An element $[a]$ of $\mathbb{Z}_n$ has multiplicative inverse if and only if $\gcd(a, n) = 1$.

The proof explains how to find the multiplicative inverse explicitly. If a is an integer such that $\gcd(a, n) = 1$ (which one can check in practice by Euclid's algorithm), Euclid's algorithm find integers b and c such that $ab + nc = \gcd(a, n) = 1$. It then follows that $ab \equiv 1 \bmod n$, i.e. $[a][b] = [ab] = [1]$.

Proposition 13. An element $[a]$ of $\mathbb{Z}_n$ has no multiplicative inverse if and only if there exists b, not congruent to 0 mod n, such that $[a][b] = [0]$.

Example. $[2]_6[3]_6 = [0]_6$.

It is possible to compute the number of elements in $\mathbb{Z}_n$ with multiplicative inverses, using the fundamental theorem of arithmetic: if $= \prod_p p^{r_p}$, then it is computed by $\prod_p (p-1)p^{r_p - 1}$.

What is it useful for? It is possible to solve 'linear congruence equations': $ax + b \equiv c \bmod n$ (when $\gcd(a, n) = 1$). Indeed, $[x] = [c - b][a]^{-1}$ where $[a]^{-1}$ is the multiplicative inverse of $[a]$ (this is NOT $1/[a]$). What if $\gcd(a, n) > 1$? Take Number Theory next year!