Discrete Math 37110 - Class 3 (2016-10-04)

Instructor: László Babai
Notes taken by Jacob Burroughs
Revised by instructor

3.1 Fundamental Theorem of Arithmetic (unique prime factorization)

Definition 3.1 (Prime number). p is a *prime number* if $p \geq 2$ and

$$(\forall x)(x \mid p \implies x \in \{\pm 1, \pm p\})$$

DO 3.2. Prove by induction on $n \geq 1$ that n has a prime factorization:

$$(\exists \text{ primes } p_1, \dots, p_k)(n = p_1 \cdots p_k)$$

(Note that this works for $n = 1$ as well: we set $k = 0$ and $1 = \prod_{i \in \emptyset} p_i$, since the product of the empty set is defined to be 1)

The **Fundamental Theorem of Arithmetic** states that for every $n \geq 1$, a prime factorization of n exists and is unique up to the order of the primes involved. The existence is an easy exercise (above); the essence of the theorem is uniqueness. We state the unqieness formally.

Theorem 3.3 (Uniqueness of prime factorization). *If $p_1 \cdots p_k = q_1 \cdots q_\ell$ where the p_i and q_j are prime numbers then $k = \ell$ and there is a permutation σ of the set $\{1, \dots, k\}$ (i.e., a bijection $\{1, \dots, k\} \to \{1, \dots, k\}$) such that $(\forall i)(q_i = p_{\sigma(i)})$.*

We now describe the key tool to proving the Uniqueness theorem.

Definition 3.4 (Prime Property). $z \in \mathbb{Z}$ has the *prime property* if $z \neq \pm 1$ and

$$(\forall a, b)(z \mid ab \implies (z \mid a) \vee (z \mid b))$$

Example 3.5. Show that 6 does not have the prime property.

We want to show that $(\exists a, b)(6 \mid ab \wedge (6 \nmid a) \wedge (6 \nmid b))$ Let $a = 4$, $b = 3$. Then $6 \mid 4 \cdot 3$ but $6 \nmid 4$ and $6 \nmid 3$.

DO 3.6. Prove: If z is composite (i.e. $(\exists u, v)(u, v \geq 2) \wedge z = uv$), then z does not have the prime property.

DO 3.7. Prove: 0 has the prime property.

Next we state the main technical result of today's class.

Theorem 3.8 (Prime property theorem). *All prime numbers have the prime property.*

The proof of this result will be the focus of today's lecture.

DO 3.9. Derive the Uniqueness of prime factorization theorem (Theorem 3.3) from the Prime property theorem (Theorem 3.8).

The proof of the Prime property theorem will follow from the existence and basic properties of the gcd. We shall give two proofs of the existence of gcd.

3.2 Existence of gcd via cyclicity of subgroups of $\mathbb{Z}$

Our first proof will not only establish the existence of $\gcd(a, b)$ but also that it can be represented in the form $ax + by$, i.e., as a linear combination of a and b. The latter part is often referred to as "Bézout's lemma."

Theorem 3.10 (Existence of the GCD and Bézout's lemma)**.**

$$(\forall a, b)(\exists \gcd(a, b) =: d \wedge (\exists x, y)(d = ax + by))$$

Our tool for proving this result is the fact that all subgroups of $\mathbb{Z}$ are cyclic, as stated in 2A.8HW. Recall the definition.

Definition 3.11. A non-empty subset $H \subseteq \mathbb{Z}$ is a *subgroup* of $\mathbb{Z}$ if $0 \in H$ and H is closed under subtraction ($H - H \subseteq H$). We denote this circumstance by writing $H \leq \mathbb{Z}$.

Definition 3.12. A *cyclic subgroup* is a subgroup of the form $a\mathbb{Z}$ (all multiples of a). The number a is called a *generator* of this subgroup.

Theorem 3.13 (All subgroups cyclic)**.** *All subgroups of* $\mathbb{Z}$ *are cyclic.*

DO 3.14. Derive Theorem 3.10 from the "All subgroups cyclic" theorem (Theorem 3.13.

Hint. First prove that the set of linear combinations, $a\mathbb{Z} + b\mathbb{Z} = \{ax + by \mid x, y \in \mathbb{Z}\}$, is a subgroup. Let d be a generator of this subgroup. Now prove that d satisfies the definition of a greatest common divisor of a and b.

We now discuss the proof of the "All subgroups cyclic" theorem.

Proof. From the easy part of the homework we know that:

$$\begin{aligned} a \in H &\implies -a \in H \\ 0 \in H & \\ a, b \in H &\implies a + b \in H \\ a \in H &\implies (\forall n \in \mathbb{Z})(na \in H) \\ a \in H &\implies a\mathbb{Z} \subseteq H \end{aligned}$$

Case 1: $H = \{0\}$. Then $H = 0\mathbb{Z}$.

Case 2: $H \neq \{0\}$
There exists a positive number in H. We shall call the smallest such number d. This is our suspect for a generator of H.
Claim. $H = d\mathbb{Z}$.
We already know that $d\mathbb{Z} \subseteq H$. We need to show the opposite inclusion, i.e., that $(h \in H) \implies (h \in d\mathbb{Z})$.

Let $h \in H$. By the Division Theorem (Problem 2A.2), $(\exists q, r)(h = dq + r \wedge 0 \leq r < d)$. We know that $d \in H$ implies $d\mathbb{Z} \subseteq H$, and thus $dq \in H$. But then, $r = h - dq \in H - H \subseteq H$, so $r \in H$. Now r cannot be positive since d was minimal, and therefore $r = 0$, so we proved that $d \mid h$, i.e., $h \in d\mathbb{Z}$. This completes the proof of the Claim and thereby the proof of the "all subgroups cyclic" theorem (Theorem 3.13). □

We are now just a few steps away from proving Theorem 3.10.

Lemma 3.15. *A linear combination that is a common divisor is necessarily a greatest common divisor. In other words, if $f = ax + by$ and $f \mid a$, $f \mid b$, then f is a greatest common divisor of a and b.*

Proof. Suppose that $e \mid a \wedge e \mid b$. Then $e \mid ax$ and $e \mid by$, so $e \mid ax + by = f$. □

Lemma 3.16.

$$\gcd(ad, bc) = |c| \gcd(a, b)$$

Proof. Need to show that $A = \gcd(ad, bc)$ divides $B = |c| \gcd(a, b)$ and vice versa.

First we show that $B \mid A$. This is immediate from the definition of gcd.

$$d \mid a \implies dc \mid ac$$
$$d \mid b \implies dc \mid bc$$
$$\text{Therefore, } B = dc \mid \gcd(ac, bc) = A$$

The converse, $A \mid B$, is far from evident; it will require Bézout's lemma: $\gcd(a, b) = ax + by$ for some x, y. Now $B = |c|(ax + by) = \pm(acx + bcy)$. Now $A \mid ac$ and $A \mid bc$; therefore $A \mid acx + bcy = \pm B \mid B$. □

Finally, we are ready to prove that prime numbers have the prime property (Theorem 3.8).

Proof. Suppose that p is a prime number and that $p \mid ab$ and $p \nmid b$. We then want to show that $p \mid a$.

Given $p \mid ab$ and $p \mid ap$, by the definition of gcd, $p \mid \gcd(ab, ap) = |a| \, \mathrm{g\dot{c}d}(b, p)$ by Lemma 3.16.

Since p is prime and does not divide b, $|a| \, \mathrm{g\dot{c}d}(b, p) = |a|$, so $p \mid a$.

This completes the proof of the Prime property theorem, and thereby the Uniqueness of prime factorization and with it the Fundamental Theorem of Arithmetic. □

3.3 Existence of gcd: Euclid's algorithm

We now give the second (historically first) proof of the the existence of gcd .

Euclid's proof. Let $\mathrm{Div}(a)$ denote the set of divisors of a. For instance, $\mathrm{Div}(10) = \{\pm 1, \pm 2, \pm 5, \pm 10$.

DO 3.17. $\mathrm{Div}(a) = \mathrm{Div}(-a)$

Let $\mathrm{Div}(a, b)$ denote the set of common divisors of a, b, i.e., $\mathrm{Div}(a, b) = \mathrm{Div}(a) \cap \mathrm{Div}(b)$

DO 3.18. Euclid's Lemma: $\mathrm{Div}(a, b) = \mathrm{Div}(a - b, b)$

DO 3.19. $\mathrm{Div}(a, b) = \mathrm{Div}(a + b, a)$

DO 3.20. $\mathrm{Div}(a, b) = \mathrm{Div}(b, a)$

DO 3.21. $\mathrm{Div}(a, b) = \mathrm{Div}(a - qb, a)$ for all q

DO 3.22. $\mathrm{Div}(a, 0) = \mathrm{Div}(a)$.

Hint. $\mathrm{Div}(0) = \mathbb{Z}$.

DO 3.23. d is a greatest common divisor of a, b exactly if $\mathrm{Div}(a, b) = \mathrm{Div}(d)$

Euclid's proof is algorithmic, it goes via "Euclid's algorithm." We already know that $\gcd(a, 0) = |a|$ $\gcd(\pm a, \pm b) = \gcd(|a|, |b|)$ assuming the right hand side exists, so it suffices to show that every pair of positive integers has a gdc. We describe the algorithm in *pseudocode*.

Euclid's algorithm

Input: integers $a \geq b > 0$

Output: $\gcd(a, b)$

Auxiliary variables (updated in every round): integers $A > B \geq 0$

Loop invariant: throughout the algorithm we shall maintain $\mathrm{Div}(A, B) = \mathrm{Div}(a, b)$

```
initialize:   $A \leftarrow a$, $B \leftarrow b$
while $B > 0$
   let $A = Bq + r$ where $0 \leq r < B$ (Division Theorem)
   let $A \leftarrow B$ and $B \leftarrow r$
end(while)
return $A$
```

DO 3.24. Use Euclid's algorithm to find $\gcd(897, 644)$. Do not use electronic devices.

DO 3.25. Prove that the algorithm terminates in a finite number of steps.

Hint. Show that the value of B goes down in every round.

DO 3.26. Verify the Loop invariant.

Hint. Euclid's lemma.

DO 3.27. Prove that the value d returned satisfies $\mathrm{Div}(d) = \mathrm{Div}(a, b)$.

Hint. At the time of exit from the "while" loop we have $B = 0$ and therefore $\text{Div}(A, B) = \text{Div}(A)$. But d is the value of A at this point.

DO 3.28. Prove that the value d returned is $\gcd(a, b)$.

Hint. Exercise 3.23.

This completes the justification of Euclid's Algorithm and thereby Euclid's proof of the existence of gcd. □

DO 3.29. Use Euclid's proof to prove that the gcd is a linear combination.

3.4 Multiplicative inverse

Definition 3.30. x is a multiplicative inverse of $a \mod m$ if $ax \equiv 1 \mod m$

Theorem 3.31. *$\underline{a}$ has a multiplicative inverse* $\mod m$ *if and only if $\underline{a}$ and m are relatively prime, i.e.,* $\gcd(a, m) = 1$.

DO 3.32. If $d \mid m$ and $a \equiv b \pmod{m}$ then $a \equiv b \pmod{d}$.

Proof of Theorem 3.31. First, let us show that, assuming $\gcd(a, m) = 1 \mod m$, a multiplicative inverse exists. This follows from Bézout's Lemma: $1 = ax + my$, so $1 \equiv ax \pmod{m}$.

Assume now that a multiplicative inverse exists. We must show that $\gcd(a, m) = 1 \pmod{m}$. This is easier: it follows from the definition of gcd. Indeed, let $d = \gcd(a, m)$. Then $d \mid m$, so by exercise 3.32, we have $ax \equiv 1 \pmod{d}$. But $d \mid a$, i.e., $a \equiv 0 \pmod{d}$, so $ax \equiv 1 \pmod{d}$ translates to $0 \equiv 1 \pmod{d}$ and therefore $d \mid 1$. □

Example 3.33. We demonstrate how to find the multiplicative inverse of 6 modulo 17.

$$\begin{aligned} 6x &\equiv 1 \pmod{17} \\ 17x &\equiv 0 \pmod{17} \\ 12x &\equiv 2 \pmod{17} \\ 5x &\equiv -2 \pmod{17} \\ x &\equiv 3 \pmod{17} \end{aligned}$$

The third line is twice the first line. The fourth line is the second minus the third. The fifth line is the first minus the fourth. What this procedure proves is that the only possible inverses of 6 modulo 17 are the numbers $\equiv 3 \pmod{17}$. The fact that these actually work follows from Theorem 3.31 since 6 and 17 are relatively prime.

Note that we essentially performed Euclid's algorithm on the coefficients on the left-hand side.

The multiplicative inverse is not unique.

DO 3.34. Prove that the multiplicative inverse is unique modulo m. This means the following. Assume x is a multiplicative inverse of a modulo m. Then a number y is a multiplicative inverse of a modulo m if and only if $y \equiv x \pmod{m}$.

So we can talk about multiplicative inverses among residue classes. Notation for the previous example:

$$[6^{-1}]_{17} = [3]_{17}.$$