MATH 417

Iwan Duursma

January 21, 2022

Week 1 - Friday

Course outline

Math 417 Introduction to Abstract Algebra [43 hrs]

(a) Integers [4 hrs]

(b) Permutations [3hrs]

(c) Groups [10 hrs]

(d) Group actions [10 hrs]

(e) Rings [12 hrs]

(*) Exams and leeway [4hrs]

(a) Integers [4hrs]

[Rotman-1.3-1.5]

The Integer division algorithm (p.35) - We 1/19

optional: Euclidean algorithm (pp.43-45) - We 1/19, Fr 1/21

Greatest common divisor (pp.37-38) - We 1/19

Fundamental theorem of arithmetic (pp.53-55) - Fr 1/21

Congruence arithmetic (pp.57-59) - Mo 1/24

optional: Application to RSA-cryptosystem (handout or homework)

Lemma

Let $b = q \cdot a + r$. Then $\gcd(b, a) = \gcd(a, r)$.

Proof

The pair b, a has the same set of common divisors as the pair a, r.

To compute $\gcd(119, 301)$ we use the lemma repeatedly.

$$
\begin{array}{rclrl}
 & & & & d = \gcd(301, 119) \\
301 & = & 2 \cdot 119 + & 63 : & = \gcd(119, 63) \\
119 & = & 1 \cdot 63 + & 56 : & = \gcd(63, 56) \\
63 & = & 1 \cdot 56 + & 7 : & = \gcd(56, 7) \\
56 & = & 8 \cdot 7 + & 0 : & = \gcd(7, 0) = 7
\end{array}
$$

Extended Euclidean algorithm

Theorem : Let $d = \gcd(a, b)$. Then d is of the form

$$d = sa + tb,$$

where s and t are integers (called Bézout coefficients).

Proof: After the example.

Example: $7 = \gcd(301, 119)$. What are the integers s and t such that

$$7 = 301s + 119t \ ?$$

Bézout coefficients for $(301, 119)$

$$
\begin{array}{rcrcrcrcrcr}
301 &=& 2 \cdot 119 &+& 63 &:& 63 &=& 301 &-& 2 \cdot 119. \\
119 &=& 1 \cdot 63 &+& 56 &:& 56 &=& 119 &-& 1 \cdot 63. \\
 && && && &=& -301 &+& 3 \cdot 119. \\
63 &=& 1 \cdot 56 &+& 7 &:& 7 &=& 63 &-& 1 \cdot 56. \\
 && && && &=& 2 \cdot 301 &-& 5 \cdot 119. \\
56 &=& 8 \cdot 7 &+& 0 && && && &
\end{array}
$$

Remark: We compute s and t working from the top down.

Example 1.42 in Rotman is slighly different and works from the bottom up.

Same procedure, formatted as a table

	q	r	s	t
-1		301	1	0
0	2	119	0	1
1	1	63	1	-2
2	1	56	-1	3
3	8	7	2	-5

Proof that $d = \gcd(a, b)$ is of the form $sa + tb$

We may assume that $0 \leq a \leq b$.

For $a = 0$ (and $b \neq 0$), $d = b = 0 \cdot a + 1 \cdot b$.

For $a > 0$, let $b = qa + r$ with $0 \leq r < a \leq b$. Then

$$\begin{aligned} & d \in \{sa + tb \ : \ s, t \in \mathbb{Z}\} \\ \Leftrightarrow \ & d \in \{sa + t(qa + r) : s, t \in \mathbb{Z}\} \\ \Leftrightarrow \ & d \in \{(s + tq)a + tr) : s, t \in \mathbb{Z}\} \\ \Leftrightarrow \ & d \in \{tr + ua : t, u \in \mathbb{Z}\}. \end{aligned}$$

Apply this to each step in $\gcd(b, a) = \gcd(a, r) = \cdots = \gcd(d, 0)$.

$$\begin{aligned} \{sa + tb \ : \ s, t \in \mathbb{Z}\} \ &= \ \{tr + ua : t, u \in \mathbb{Z}\} \ = \ \cdots = \\ &= \ \{x \cdot 0 + y \cdot d : x, y \in \mathbb{Z}\} \ = \ \{\ldots, -2d, -d, 0, d, 2d, \ldots\}. \end{aligned}$$

Least Integer Axiom

There is a smallest integer in every nonempty subset S of the natural numbers $\mathbb{N} = \{0, 1, 2, \ldots\}$.

(Also known as the Well-Ordering Principle)

Existence of prime factorizations

Theorem

Every integer $n \geq 2$ is either a prime or a product of primes.

Proof

Let $S \subset \mathbb{N}$ be the set of all n without the given property.

Assume that S is nonempty. Then S contains a least element m.

Since m is not a prime it can be written as $m = ab$ with $1 < a, b < m$.

But then $a, b \notin S$ shows that m is a product of primes. Contradiction.

Thus $S = \emptyset$.

Fundamental Theorem of Arithmetic

Theorem

Every integer $n \geq 2$ has a unique factorization as a product of primes.

Proof

With the previous theorem it remains to prove uniqueness.

Let $a = p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n$ be two factorizations of the integer a into products of primes. The right hand side is divisible by p_m. But then $q_i = p_m$ for some i. After cancellation of p_m and q_i we are left with a smaller number of prime factors. The claim follows by induction.

p divides $q_1 q_2 \cdots q_n$

The proof uses that $q_i = p$ for some i when the prime p divides $q_1 q_2 \cdots q_n$.

Assume that $q_n \neq p$. Then $\gcd(q_n, p) = 1$ and there exist Bézout coefficients s and t such that $1 = sq_n + tp$.

Multiplying both sides by $q_1 q_2 \cdots q_{n-1}$,

$$q_1 q_2 \cdots q_{n-1} = sq_1 q_2 \cdots q_n + tq_1 q_2 \cdots q_{n-1} p.$$

Since both terms on the right are divisble by p, so is $q_1 q_2 \cdots q_{n-1}$.

If $q_i \neq p$ for all i a repeated application would lead to p divides 1.