MA341 Number Theory
Kalin Kostadinov

Lecture 3 (29 May 2008)

Divisibility, Factoring, Primes. The Fundamental Theorem of Arithmetic.

Overview. The goal of this lecture is to provide a proof of the Fundamental Theorem of Arithmetic, which states that every positive integer greater than 1 could be decomposed, in an essentially unique way, as product of prime numbers. To this end, we first built the solid foundation that underlies all proofs, and list the axioms of the integers we distilled in our first workshop. Then we introduce the simple division with remainder property and discuss the prime numbers, before finally proving the Fundamental Theorem.

WOP and PMI. These are the abbreviations for the Well Ordering Principle and the Principle of Mathematical Induction, two equivalent forms of the axiom of the system of the integers, $\mathbb{Z}$ that distinguishes it from all the other rings. Let us list all the axioms we discussed during the workshop:

1. $\mathbb{Z}$ is closed under two operations, " $+$ " and "$\cdot$"
2. Both "$+$" and "$\cdot$" are commutative and associative.
3. The distributive law hold: $a(b+c) = ab + ac$, $\forall a, b, c \in \mathbb{Z}$.
4. In $\mathbb{Z}$ there is a neutral element with respect to " $+$ ", denoted 0, such that $a + 0 = a$, $\forall a \in \mathbb{Z}$.
5. In $\mathbb{Z}$ there is a neutral element with respect to "$\cdot$", denoted 1, such that $a \cdot 1 = a$, $\forall a \in \mathbb{Z}$.
6. Every element $a \in \mathbb{Z}$ has an additive inverse, i.e. there is $a' \in \mathbb{Z}$ such that $a + a' = 0$.
7. PMI: $\mathbb{Z}$ has a distinguished subset, the natural numbers, denoted $\mathbb{N}$, and defined by the three properties:
   - $1 \in \mathbb{N}$
   - If $n \in \mathbb{N}$ then $n + 1 \in \mathbb{N}$.
   - Every element in $\mathbb{N}$ is obtained by one of these two rules.
8. (Trichotomy) For any $a \in \mathbb{Z}$, exactly one of these three options hold:
   - $a = 0$;
   - $a \in \mathbb{N}$;
   - $-a \in \mathbb{N}$;

The Well Ordering Principle states that every non-empty set of positive integers has a minimal element, i.e. if $S \subseteq \mathbb{N}$ is non-empty, then $\exists a \in S$ such that for every other $b \in S, a < b$. It is equivalent to PMI. Indeed, let S be a non-empty set of positive integers, which has no least element. This means that there is a infinite decreasing sequence $a_1 > a_2 > a_3 \dots$ of elements of S. But every element of S is a positive integer, in particular $a_1 \in \mathbb{N}$ and by PMI there are only finitely many positive integers smaller than a_1, contradiction. Therefore PMI implies WOP. We don't need the implication in the other direction, so will skip its proof.

The Division Algorithm and the Euclidean Algorithm. The Well Ordering Principle is the main ingredient in the proof of the following statement:

Theorem. Given arbitrary $a, b \in \mathbb{N}$ there exists unique non-negative integers q and$r$, such that $a = bq + r$ and $0 \leq r < b$.

Proof. Let $S = \{a - bs | s \in \mathbb{Z}, a - bs \in \mathbb{N}\}$. This set is non-empty, since for example it contains $a = a - b \cdot 0$, and hence by WOP it has a minimal element. Call it r, and the value of s for which it is obtained call q. Then $a = bq + r$ for non-negative integers q, r and if $r > b$ then $a - b(q-1) = r - b$ is also in S in contradiction of the choice of r to be the smallest element of S. Hence $0 \leq r < b$ as needed. For the uniqueness, let q, r and q', r' have the desired properties. Then $b(q - q') = r - r'$, so $b | r - r'$, while $|r - r'| < b$, so $r = r'$ and then $q = q'$ as well. □

Repetitive use of the above division algorithm is the ingredient of the famous Euclidean algorithm. Let a, b be positive integers. Do the divisions

$$\begin{aligned} a &= bq_1 + r_1 & 0 \leq r_1 \leq b \\ b &= r_1 q_2 + r_2 & 0 \leq r_2 \leq r_1 \\ r_1 &= r_2 q_2 + r_3 & 0 \leq r_3 \leq r_2 \\ &\vdots & \vdots \end{aligned}$$

In this way we get a decreasing sequence of remainders

$$b > r_1 > r_2 > r_3 > \cdots \geq 0$$

so eventually there is an index k such that $r_{k+1} = 0$, and the last division looks like $r_k - 1 = r_k q_k$. The output of the algorithm is r_k, the last non-zero reminder.

Definition. Given two arbitrary positive integers a and b, we define their *greatest common divisor* to be r_k, the output of the Euclidean algorithm with inputs a and b. With denote the greatest common divisor by $\gcd(a, b)$.

Looking backwards in the Euclidean algorithm, we see from $r_{k-1} = r_k q_k$ that $r_k | r_{k-1}$, then from the previous line $r_{k-2} = r_{k-1} q_{k-1} + r_k$ that now $r_k | r_k - 2$, going up we see that ultimately $r_k | b$ and from the first line then that $r_k | a$.

Moreover, again going backwards, we express

$$\begin{aligned} r_k &= r_{k-2} - r_{k-1}q_{k-1} = r_{k-2} - (r_{k-3} - r_{k-2}q_{k-2})q_{k-1} = \\ &= u_{k-2}r_{k-2} + v_{k-3}r_{k-3} = \cdots = u_{k-3}r_{k-3} + v_{k-4}r_{k-4} = \dots \\ &= ua + vb \end{aligned}$$

which means that $\gcd(a,b)$ could always be expressed as a linear combination of a, b with some integer coefficients u, v. (Do an example for yourself and you will see it more clearly.) It is also clear that every number that divides both a and b also divides any linear combinations of a and b, so at the end divides $\gcd(a,b)$. We put this three important properties together in the next theorem:

Theorem. The greatest common divisor $d = \gcd(a,b)$ of two positive integers a and b has the following three properties:

1. $d|a$ and $d|b$.
2. There exists integers u and v such that $d = ua + vb$.
3. If a number d' has the properties that $d'|a$ and $d'|b$, then $d'|d$ as well.

The first and the third of these properties are characteristic for the $\gcd(a,b)$, i.e. if a number satisfies them it also satisfies the second property and is the unique output of the Euclidean algorithm for a and b.

Prime numbers. Not all numbers are created equal. A chocolate box often contains 24 candies, and very rarely 23. The reason behind this is that 24 pieces could be equally divided between 2 kids, or 3 kids, or $4, 6, 8$, even 12, while 23 cannot be split non-trivially into equal parts. This property of 23 to be indecomposable is shared with other numbers, like $2, 3, 5, 7, 11, 13, 17, 19, 23, 29$ to name just the first few. These numbers have a special name.

Definition. A positive integer $p > 1$ is called *prime* when the only two positive number that divide it are 1 and p itself. A positive integer greater than 1 which is not prime is called *composite*.

According to that definition, a positive integer is either prime, composite, or equal to 1.
There are infinitely many primes, as we shall see in the next lecture.

The Fundamental Theorem of Arithmetic. Let $n > 1$ be an integer. Then there exist a positive integer k, primes$p_1, p_2, \dots, p_k$ and positive numbers $e_1, e_2, \dots, e_k$ such that $n = p_1^{e_1}p_2^{e_2}\dots p_k^{e_k}$. The number k, the list of primes, and the exponents associated to them are uniquely determined by n.
Note that this theorem has two parts, an existence statement, and an uniqueness statement. The latter one, may be surprisingly, is a much deeper property. To prove the existence of a factorization, assume that there are some positive integers, greater than 1, that don't posses one. By the WOP then there is a smallest such integer, call it m. It cannot be a prime, since a prime is its own decomposition into primes, i.e. $k = 1, p_1 = m, e_1 = 1$. Therefore m is composite, so there exists numbers a and b, $1 < a, b < m$ such that $m = ab$. Because of

the choice of m to be the smallest integer for which the factorization fails, both a and b are products of primes. But then so is clearly m, a contradiction, due to the assumption that there are numbers that don't posses a factorization into primes.

To prove the uniqueness of a factorization, we first note that if a p is prime, and a is an arbitrary integer, then either $p|a$ or p and a are relatively prime. In the second case, the Euclidean algorithm gives us two integers, u, v such that $pu + av = 1$. So we could record the following important property,

Theorem. If a prime p divides the product ab, then it divides at least one of the factors, $p|a$ or $p|b$.

Indeed, if $p|ab$ and p does not divide a for example, then by the above $1 = pu + av$, so $b = pub + abv$, and since p divides the right hand side of the last equality, it must divide b.

This theorem is the heart of the proof of the uniqueness of factorization. For simplicity, we do just the case of a product of two primes, the general case is similar, but with more cumbersome notation.

Let $n = p_1p_2 = q_1q_2$. Then $p_1|q_1q_2$, which implies that $p_1|q_1$ or $p_1|q_2$. In the first case $p_1 = q_1$ and $p_2 = q_2$, while in the second case $p_1 = q_2$ and $p_2 = q_1$. Therefore in both cases the two factorization are identical, as claimed.