ELEMENTARY NUMBER THEORY

DIEGO CHICHARRO GORDO – LECTURE 1

v.0.3

CONTENTS

1. THE BASIS REPRESENTATION THEOREM

Theorem 1. *Let $k > 1$ be an integer. For each positive integer n there exists a unique representation to base k, this is, exist positive integers $a_0, a_1, a_2, \dots, a_h$ such that*

$$n = a_0 + a_1 k + a_2 k^2 + \cdots + a_h k^h$$

and are unique.

Proof. Let $r(n)$ the number of representations of n to base k (note that $r(n)$ can be zero), we have to show that $r(n) = 1$ for each n. If we prove that given a representation of n, we can find a representation of $n-1$, then it follows by induction that $r(n) \leq r(m)$ for each pair of integer $n > m$. Thus, we have that

$$1 = r(1) \geq r(n) \geq r(k^n) = 1$$

for if $k > 1$, then $n < k^n$, and hence $r(n) = 1$ for each n. To show that $r(n) \leq r(n-1)$, write $na_s k^s + \cdots + a_h k^h$, where a_s is the first non-zero digit starting from the right, and thus

Date: August 4, 2016.

subtracting 1 in both sides we obtain

$$\begin{aligned} n-1 &= a_m k^m + a_{m-1}k^{m-1} + \cdots + a_s k^s \\ &= a_m k^m + a_{m-1}k^{m-1} + \cdots + \big(a_s - 1\big)k^s + k^s - 1 \\ &= a_m k^m + a_{m-1}k^{m-1} + \cdots + \big(a_s - 1\big)k^s + \sum_{j=0}^{s-1}(k-1)k^j, \end{aligned}$$

where we have used the equality

$$(1+x+x^2+\cdots+x^n)(x-1) = x^{n+1}-1.$$

Thus, we have found a representation of $n-1$ as each coefficient is greater or equal than zero. This concludes the proof. □

2. Euclid's Division Lemma

Theorem 2. *For each pair a,b of integers exists a unique pair q,r (q is the* ***quotient*** *and r the* ***remainder****) of positive integers such that $0 \le r < b$ such that $a = bq + r$.*

Proof. For the existence we induct on a. Firstly consider $a \ge 0$. The base case $a = 0$ holds as $0 = 0 \cdot b + 0$. Suppose $a = bq + r$, we have to show that exists a pair q', r' such that $a + 1 = bq' + r'$ with $0 \le r' < |b|$. But

$$a+1 = bq + \big(r+1\big),$$

so if $r+1 < b$, $q' := q$ and $r' := r+1$ do the job, and if $r+1 = b$, $q' = q+1$ and $r = 0$. With the same reasoning we can conclude the same for $a < 0$ considering its opposite $-a$.

To prove the uniqueness, suppose $b = aq + r = aq' + r'$, then $a(q - q') = 0$, and thus $q = q'$, as $a \ne 0$. This leads to $r = r'$. □

3. Basic concepts on divisibility

Definition 3. Let a,b be integers, we say that a **divides** b, and we write $a|b$, if and only if there exists an integer c such that $b = ac$. For example, $3|6$ and $10|100$. If a does not divide b, we write $a \nmid b$. For example, $3 \nmid 5$.

Proposition 4 (Properties of divisibility)**.**

(1) $a|a$. *(Reflexive property)*
(2) If $a|b$ *and* $b|c$*, then* $a|c$. *(Transitive property)*
(3) If $a|b$ *and* $a|c$*, then* $a|bn+cm$ *with* m,n *integers.* *(Linearity property)*
(4) If $a|b$*, then* $ac|bc$. *(Multiplication property)*
(5) If $ac|ac$ *and* $a \ne 0$*, then* $b|c$. *(Cancelation law)*
(6) $1|a$. *(1 divides every integer)*
(7) $a|0$. *(Every integer divides zero)*
(8) $0|a$ *implies* $a = 0$. *(Zero divides only zero)*

(9) *$a|b$ implies $|a| \leq |b|$.* *(Comparison property)*
(10) *$a|b$ and $b|a$ implies $|a| = |b|$.*
(11) *$a|b$ and $a \neq 0$ implies $(b/a)|b$.*

Proof. Left as exercise. □

Definition 5. Let a,b two integers, the **greatest common divisor** of a and b is defined as the unique[1] positive integer d such that $d|a$, $d|b$ and if c divides a and b, then $c|d$. It is denoted as $\gcd(a,b)$ or (a,b). In general, given integers $a_1,a_2,\dots,a_n$, the greatest common divisor is defined as the positive integer d such that d divides all $a_1,a_2,\dots,a_n$, and $c|d$ for each integer c that divides $a_1,a_2,\cdots,a_n$. It is denoted as $\gcd(a_1,a_2,\dots,a_n)$ or $(a_1,a_2,\dots,a_n)$. For example, $(3,5) = 1$, meanwhile $(10,5) = 5$ and $(12,8) = 4$.

Proposition 6 (Properties of the gcd)**.**

(1) *$(a,b) = (b,a)$.* *(Commutative law)*
(2) *$(ac,bc) = |c|(a,b)$.* *(Distributive law)*
(3) *$(a,1) = 1$, $(a,0) = |a|$.*
(4) *$(a,b) \geq 0$ and $(a,b) = 0$ iff both $a = 0$ and $b = 0$.*

Definition 7. Given integers a,b, the **least common multiple** e is defined as the smallest integer such that a and b divides e. We'll denote it as $\operatorname{lcm}(a,b)$ or $[a,b]$. Of course, if $a_1,a_2,\cdots,a_n$ are integers, $e := [a_1,a_2,\cdots,a_n]$ verifies that is the smallest integer such that a_i divides e for each i. For example, $[10,20] = 20$ and $[12,8] = 24$.

Lemma 8. *If $a = bq + r$, then $(a,b) = (b,r)$.*

Proof. Let $d := (a,b)$ and $d' := (b,r)$. Since $d|a$ and $d|b$, we know that $d|a - bq = r$, so $d|d'$. Similarly, $d'|d$, and thus $d = d'$. □

Proposition 9 (Euclidean Algorithm)**.** *Using previous lemma we'll lead within a finite number of steps to an equality $(a,b) = (\mathfrak{r},0) = \mathfrak{r}$.*

Proof. We have that $(a,b) = (b,r) = (r,r') = \cdots$ where $a = bq + r$, $b = rq' + r'$ and so on. Since $r > r' > \cdots$ is a strictly decreasing sequence bounded above by zero, necessarily the process is finite and ends with $(\mathfrak{r},0)$. □

Theorem 10 (Bezout's Theorem)**.** *Let a and b be integers, there exists integers c and d such that $ac + bd = (a,b)$.*

Proof. If $a = b$, then $(a,b) = a = a + 0 \cdot b$. Suppose $a > b \geq 0$, we induct on $a + b$. The base case holds as $(1,0) = 1 + 0$. Suppose the result holds for every $a + b < n$, we have to show that it holds for $a + b = n$. Write $a = bq + r$, then $(a,b) = (b,r)$ and $b + r < a + b = n$, and thus by hypothesis exist x and y such that $(b,r) = yb + xr$. Hence,

$$(a,b) = ax + b(y - xq).$$

[1] Exercise: show why it is unique.

Setting $y' := y - xq$ we finish the inductive argument.

If a or b is negative, it suffices to consider $-x$ or $-y$ instead of x and y respectively. $\square$

4. Prime numbers

Definition 11. We say that two integers a and b are **relatively prime** if $(a,b) = 1$. For example, 6 and 13 are relatively prime, as $(6,13) = 1$. If an integer $p > 1$ is such that $(p,a) = 1$ for each positive integer a, we say that p is **prime**. For example, 13 is prime. If a number is not prime, then is **composite**.

Theorem 12 (Euclid's Lemma)**.** *If $a|bc$ and $(a,b) = 1$, then $a|c$.*

Proof. If $(a,b) = 1$ then exist integers x and y such that $ax + by = 1$, and thus
$$a|axc + byc = c(ax + by) = c.$$
$\square$

Theorem 13. *There are infinitely many primes.*

Proof (Euclid). If $p_1, p_2, \ldots, p_k$ are all the primes, then $P := p_k! + 1 > p_k$ is prime, for if $p|P$, then $p|1$, and thus $p = 1$, contradiction. $\square$

Proof (Euler). Let $S = 1 + 1/2 + 1/3 + 1/4 + \cdots$ be the sum of the reciprocals of all positive integer numbers. Then $S - S/2 = S(1 - 1/2)$ is the sum of the reciprocals of all the numbers that are not multiples of 2, $S(1 - 1/2) - S(1 - 1/2)/3 = S(1 - 1/2)(1 - 1/3)$ the sum of the reciprocals of all positive integers that are not multiples of 2 and 3, and in general $S(1 - 1/2)(1 - 1/3)\cdots(1 - 1/p)$ the sum of the reciprocals of all the numbers that are not multiples of each prime $q \leq p$, where p is prime. Since each number not 1 is multiple of a prime, we have that
$$S\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\cdots\left(1 - \frac{1}{p}\right)\cdots = 1,$$
or
$$S = \left(1 - \frac{1}{2}\right)^{-1}\left(1 - \frac{1}{3}\right)^{-1}\cdots\left(1 - \frac{1}{p}\right)^{-1}\cdots.$$
Since S is divergent, the product must be infinite, and thus there are infinitely many primes. $\square$

5. The Fundamental Theorem of Arithmetic

Theorem 14 (FTA)**.** *Every positive integer n is either prime or can be uniquely factorized by product of primes.*

Proof. First the existence by strong induction. The base case $n = 2$ is prime. Suppose all $1, 2, 3, \cdots, n - 1$ are either primes or product of primes. If n is prime, we're done. If not, there exists a and b less than n and greater than 1 such that $n = ab$. Since a and b are primes or product of primes, by hypothesis, so is n.

Now the uniqueness. Suppose $n = p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_s$ and $m \leq s$. Since p_i divides $q_1 q_2 \cdots q_s$ for each i, by Euclid's Lemma there exists a q_j such that $p_i | q_j$, and thus $p_i = q_j$, for both are primes. Then, dividing n by each p_i, if $m < s$ we have that

$$1 = q_{a_1} q_{a_2} \cdots q_{a_k} > 1,$$

what is impossible. Hence $m = s$ and for each i exists a j such that $p_i = q_j$. □

Proposition 15. *Let a, b be integers such that $a = \prod_p p^{a_p}$ and $b = \prod_p p^{b_p}$, then*

$$\gcd(a,b) = \prod_p p^{c_p} \text{ and } \operatorname{lcm}(a,b) = \prod_p p^{d_p}$$

where $c_p := \min\{a_p, b_p\}$ and $d_p := \max\{a_p, b_p\}$.

References

[1] George E. Andrews, *Number Theory*, Dover, 2000.