MATHEMATICS AROUND US – TUTORIAL AND HOMEWORK 1

Please submit all exercises below in hard copy (either in English or in Hebrew) next Thursday, November 9^{th}, in the tutorial. Sections marked as bonus are not mandatory.

1. Division with remainder

Definition: given two integers a, b where $b \neq 0$ we say that q and r are the quotient and the remainder of the division of a in b (respectively) if $a = bq + r$ and $0 \leq r < |b|$.

Example: The quotient and the remainder of the division of -55 in -6 are 10 and 5 (respectively).

Claim: For any two integers a, b where $b > 0$ there exist integers q and r such that $a = bq + r$ and $0 \leq r < b$.

Proof: Assume $b > 0$ (the proof for negative b is similar). Let us look at all the numbers of the form $\{a - xb\}_{x \in \mathbb{Z}}$. This set contains non negative numbers, so take r to be the minimal non negative number in this set. To show that $0 \leq r < b$ we assume otherwise, i.e. assume $r \geq b$. In that case $r - b = a - xb - b = a - (x+1)b \geq 0$ is a smaller non negative number in that set, a contradiction. □

1.1. Exercise: Proof that the quotient and the remainder of the division of two integers are unique, i.e. show that if a and $b \neq 0$ are two integers, $a = bq + r$ and $0 \leq r < |b|$, and also $a = bq_1 + r_1$ and $0 \leq r_1 < |b|$, then $q = q_1$ and $r = r_1$.

Definition: given two integers a, b where $b \neq 0$ we say that a is divisible by b and that b divides a if the remainder of the division of a in b is zero. In that case we write $b|a$.

2. Arithmetic Modulo N

Definition: given an integer $N > 0$ and integers a, b, we say that a and b are congruent (or equal) modulo N if $N|(a - b)$. In that case we write $a \equiv b \ (mod\ N)$.

Examples: $1 \equiv 8 \ (mod\ 7)$, $3 \equiv -97 \ (mod\ 50)$, $a \equiv b \ (mod\ 2)$ if and only if a and b have the same parity (i.e. either both are even or both are odd).

Notation: the remainder of the division of a in N is called the residue of a modulo N (and it is of course congruent to a modulo N).

2.1. Exercise: Fix $N > 0$. Prove that congruence modulo N is an equivalence relation on the integers, i.e. show that:

2.1.1. *Reflexivity.* For any integer a: $a \equiv a \ (mod\ N)$.

2.1.2. *Symmetry.* For any two integers a, b: if $a \equiv b \ (mod\ N)$ then $b \equiv a \ (mod\ N)$.

2.1.3. *Transitivity.* For any three integers a, b, c: if $a \equiv b \ (mod\ N)$ and $b \equiv c \ (mod\ N)$ then $a \equiv c \ (mod\ N)$.

Date: November 2^{nd} 2017.

2.2. Exercise: Prove that arithmetic module N is well-defined: if $a \equiv b\ (mod\ N)$ and $c \equiv d\ (mod\ N)$, then $a + c \equiv b + d\ (mod\ N)$ and $ac \equiv bd\ (mod\ N)$.

Remark: by induction one can easily show that for any $m \geq 1$: if $\{a_i \equiv b_i\ (mod\ N)\}_{i=1}^{m}$ then $\sum_{i=1}^{m} a_i \equiv \sum_{i=1}^{m} b_i\ (mod\ N)$ and $\prod_{i=1}^{m} a_i \equiv \prod_{i=1}^{m} b_i\ (mod\ N)$.

2.3. Exercise: What is the residue of 19^{101} modulo 18? What is the residue of 19^{101} modulo 20? What is the residue of 2^{100} modulo 5?

2.4. Exercise: Prove that 9 divides $2222^{7777} + 7777^{2222}$ (hint: what does it mean to be divisible by N in terms of arithmetic modulo N?).

2.5. Exercise: Let $c, N > 0$ be two positive integers, and let a, b be integers. Assume $ac \equiv bc\ (mod\ Nc)$. Prove that $a \equiv b\ (mod\ N)$.

3. Divisibility Rules

In this section we will use modular arithmetic in order to prove some divisibility rules.

3.1. Exercise: Let a be a positive integer. Assume its decimal representation is $a_k a_{k-1} a_{k-3} ... a_2 a_1$, i.e. $a = \sum_{i=1}^{k} a_i 10^{i-1}$. Denote by S the sum of a's digits in the decimal representation, i.e. $S = \sum_{i=1}^{k} a_i$. Denote by T the alternating sum of a's digits in the decimal representation, i.e. $T = \sum_{i=1}^{k} (-1)^{i+1} a_i$. Prove that:

3.1.1. $a \equiv S\ (mod\ 9)$. Deduce that a is divisible by 9 if and only if S is divisible by 9 (hint: what does it mean to be divisible by N in terms of arithmetic modulo N?).

3.1.2. $a \equiv S\ (mod\ 3)$. Deduce that a is divisible by 3 if and only if S is divisible by 3 (hint: using the previous result this is very easy).

3.1.3. (bonus) $a \equiv T\ (mod\ 11)$. Deduce that a is divisible by 11 if and only if T is divisible by 11.

4. Greatest Common Devisor

Definition: let a, b be two integers. An integer d is called a common divisor of a and b if both a and b are divisible by d.

Definition: let a, b be two integers, where at least one of them is not zero. The maximal common devisor of a and b is called the Greatest Common Divisor of a and b, and is denoted by $gcd(a, b)$. If $gcd(a, b) = 1$ we say that a and b are co-prime, or relatively prime. In that case we also say that a is co-prime to b.

Examples: $gcd(4, 6) = 2$, $gcd(125, 100) = 25$, for any non zero integer a: $gcd(a, 0) = |a|$, a prime number p is co-prime to any number which is not a multiple of it.

5. Euclid's algorithm

Given two integers a and b, where at least one of them is not zero, we would like to find $gcd(a, b)$. Thus the input of the algorithm consists of two integers a and $b \neq 0$, and the output is $gcd(a, b)$.

Description of the algorithm:

Stage 0: divide a in b:

$$a = q_0 b + r_0$$

stage 1: divide b in r_0:

$$b = q_1 r_0 + r_1$$

stage 2: divide r_0 in r_1:

$$r_0 = q_2 r_1 + r_2$$

stage 3: divide r_1 in r_2:

$$r_1 = q_3 r_2 + r_3$$

stage k: divide r_{k-2} in r_{k-1}:

$$r_{k-2} = q_k r_{k-1} + r_k$$

If $r_0 = 0$ then $gcd(a, b) = |b|$. Otherwise:

If $r_k \neq 0$ proceed to step $k+1$, otherwise $gcd(a, b) = r_{k-1}$. We denote by n the minimal integer k such that $r_k = 0$, and then $gcd(a, b) = r_{n-1}$.

The special case where $r_0 = 0$, i.e. where $b|a$, should be proven separately - make sure you understand why in that case $gcd(a, b) = |b|$.

Claim: the algorithm will stop after finitely many steps.

Proof: By definition of division with remainder we have $0 \leq r_0 < b$. In addition we have $r_0 > r_1 > r_2 > ...$ and $r_i \geq 0$ for any i. Thus the series r_i is a strictly descending series of non-negative integers, and so reaching zero at some point. □

5.1. Exercise: Prove that for any two integers a, b, where at least one of them is not zero, and for any integer q: $gcd(a, b) = gcd(a, b + qa)$ (hint: show that d is a common divisor of a and b if and only if d is a common divisor of a and $b + qa$). Deduce that r_{n-1} is indeed $gcd(a, b)$.

5.2. Exercise: Prove that $gcd(a, b)$ can be written as a linear combination of a and b with integer coefficients (hint: consider the steps of Euclid's algorithm, and prove by induction that at each step, the new remainder r_i that appears in this step can be written as linear combinations of a and b with integer coefficients).

Remark: The representation of $gcd(a, b)$ as a linear combination of a and b with integer coefficients is sometimes called Bezout's identity or Bezout's Lemma. Finding this combination using the method above is sometimes called extended Euclid's algorithm.

5.3. Exercise: Prove that $gcd(a, b)$ is the minimal positive integer that can be written as a linear combination of a and b with integer coefficients (hint: prove that if d is a common divisor of a and b then d divides any linear combination of a and b with integer coefficients).

Example: Let us calculate $gcd(23, 5)$ and write it as a linear combination of 23 and 5 with integer coefficients using Euclid's algorithm:

$$23 = 4 \cdot 5 + 3$$
$$5 = 1 \cdot 3 + 2$$
$$3 = 1 \cdot 2 + 1$$
$$2 = 2 \cdot 1 + 0$$

so $gcd(23, 5) = 1$, and

$$1 = 3 - 1 \cdot 2 = 3 - 1 \cdot (5 - 1 \cdot 3) = (-1) \cdot 5 + 2 \cdot 3 = (-1) \cdot 5 + 2 \cdot (23 - 4 \cdot 5) = 2 \cdot 23 - 9 \cdot 5.$$

5.4. Exercise: Calculate $gcd(1369, 2597)$ and write it as a linear combination of 1369 and 2597 with integer coefficients using Euclid's algorithm.

5.5. **Fundamental theorem of arithmetic.** Recall the fundamental theorem of arithmetic stating any positive integer is a factor of prime numbers, and that this factorization is unique up to ordering. Taking two positive integers

$$a = p_1^{m_1} \cdot p_2^{m_2} \cdot p_3^{m_3} \cdot p_4^{m_4} \cdots \cdot p_k^{m_k}, b = p_1^{n_1} \cdot p_2^{n_2} \cdot p_3^{n_3} \cdot p_4^{n_4} \cdots \cdot p_k^{n_k}$$

where $p_1 < p_2 < p_3 < p_4 < ... < p_k$ are prime numbers and $m_1, m_2, m_3, m_4, ..., m_k, n_1, n_2, n_3, n_4, ..., n_k$ are non negative integers, one has:

$$gcd(a, b) = p_1^{min\{m_1,n_1\}} \cdot p_2^{min\{m_2,n_2\}} \cdot p_3^{min\{m_3,n_3\}} \cdot p_4^{min\{m_4,n_4\}} \cdots p_k^{min\{m_k,n_k\}}.$$

5.5.1. Warning: In order to prove the fundamental theorem of arithmetic we usually use Euclid's algorithm and Bezout's Lemma. Thus, when proving claims about Euclid's algorithm (e.g. in the exercises above) we cannot use the fundamental theorem of arithmetic.

5.5.2. Remark: Although finding the greatest common divisor using factorization may seems to be easier than Euclid's algorithm, it is not the case. Factoring a number into primes is a difficult problem (RSA is based on this fact) so Euclid's algorithm is much more efficient and commonly used.

5.6. Exercise: (bonus) We would like to bound the number of steps in Euclid's algorithm.

5.6.1. Prove that the remainders $r_1, r_2, ...$ satisfy $r_{i+2} < r_i/2$ (hint: consider separately the cases $r_{i+1} < r_i/2$, $r_{i+1} = r_i/2$ and $r_{i+1} > r_i/2$).

5.6.2. Prove that if a and b are two positive integers, $a > b$ and $b < 2^n$ then the number of steps in Euclid's algorithm for finding $gcd(a, b)$ is not more than $2n$.

6. Invertible modulo n

Definition: given a positive integer N and two integers a and b, we say that b is inverse to a modulo N if $ab \equiv 1 \ (mod\ N)$. Given a, if such a number b exists, we say that a is invertible modulo N.

6.1. Exercise: Prove that the inverse to a modulo N is well defined modulo N, i.e. if b and c are inverse to a modulo N, then $b \equiv c \ (mod\ N)$, and conversely if b is inverse to a modulo N and $b \equiv c \ (mod\ N)$ then c is also inverse to a modulo N.

Remark: by the exercise above given a which is invertible modulo N, there exists a unique inverse b such that $b \in \{1, 2, ..., N-1\}$.

6.2. Exercise: Prove that an integer a is invertible modulo N if and only if $\gcd(a, N) = 1$, i.e. a and N are co-prime (hint: first show that a is invertible modulo N if and only if 1 can be written as a linear combination of a and N with integer coefficients. Then use Bezout's Lemma and 5.3). Deduce that given a prime number p and an integer a, a is invertible modulo p if and only if $p \nmid a$.

6.3. Exercise: Is 1369 invertible modulo 2597? If not prove it. If it does find an inverse (hint: use 5.4 and 6.2).

6.4. Exercise: (bonus) Prove Wilson's theorem: For any prime number p:

$$(p-1)! = 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p-1) \equiv -1 (mod\ p).$$

Instructions: any number $a \in \{1, ..., p-1\}$ is invertible modulo p. We know that we can choose its inverse (modulo p) b such that it also belongs to the set $\{1, ..., p-1\}$. This means that we can try to divide the numbers in the set $\{1, ..., p-1\}$ into disjoint two-element sets ("pairs") $\{a,$ inverse to $a\}$. All the numbers will get into pairs except for two (who are they and why do they have no pair?). Now use the fact that the product of two numbers in such a pair is 1 modulo p to prove Wilson's theorem.

7. Euler's ϕ function

Definition: given a positive integer N we define $\phi(N)$ to be the number of positive integers less than N that are invertible modulo N (by above this is exactly the number of positive integers less than N that are co-prime to N).

7.1. Exercise: Solve section (b) of problem 2 on p. 234 in the book "Math and Technology" (hint: try counting).

8. Euler's Theorem and Fermat's little Theorem (reminder)

Euler's Theorem: Let $N > 1$ be an integer and a be an integer which is co-prime to N, then: $a^{\phi(N)} \equiv 1 \ (mod\ N)$.

A special case of Euler's Theorem is Fermat's little Theorem: Let p be a prime number and a be an integer which is not divisible by p, then: $a^{(p-1)} \equiv 1 \ (mod\ p)$.

Remark: we will prove Euler's Theorem when we discuss Group theory later on this semester. An elementary proof may be found for instance in Wikipedia.

9. Cryptography

9.1. Exercise: Solve Problem 7 on p. 235 in the book "Math and Technology".

E-mail address: ary.shaviv@weizmann.ac.il