Margaret Bilu
Office 604

Fall 2017

bilu@cims.nyu.edu

Algebra homework 2
Arithmetic on the set of integers

Notation: For a set A with a finite number of elements, we denote by $|A|$ the number of its elements.

Exercise 1. Prove the following properties:

(a) For every integer a, the integers 1, -1, a and $-a$ divide a.

(b) 0 does not divide any non-zero integer.

(c) All integers divide 0.

(d) If a, b, c are integers such that $a|b$ and $b|c$ then $a|c$.

(e) If a, b are non-zero integers, then $a|b$ and $b|a$ implies $a = b$ or $a = -b$.

Exercise 2. Give the list of the positive divisors of the following numbers:

(a) 20

(b) 57

Exercise 3. Let p be a prime number, that is, a positive number such that its only positive divisors are 1 and p. Give the list of all the positive divisors of p^2 , then of p^3. More generally, describe, in terms of p and k, the list of positive divisors of p^k for any integer $k \geq 1$.

Exercise 4. Let n be a positive integer. Show that the smallest integer $d > 1$ dividing n is a prime number.

Exercise 5. Let a, b be two integers, not both zero. Recall that in the lectures, their greatest common divisor $\gcd(a, b)$ has been defined as the largest positive number d which divides both a and b. Show that any non-zero integer e dividing both a and b divides $\gcd(a, b)$.

Exercise 6. For any integers a, b which are not both zero, prove the following properties of the greatest common divisor:

(a) $\gcd(a, b) = \gcd(b, a)$.

(b) For any integer $k \geq 1$, $\gcd(ka, kb) = k \gcd(a, b)$.

(c) If $d = \gcd(a, b)$, then there exist relatively prime integers a', b' such that $a = da'$ and $b = db'$.

(d) $\gcd(a, b) = \gcd(a + b, b)$.

(e) $\gcd(a, a + 1) = 1$

(f) For any integer $k \geq 1$, $\gcd(a, a + k)$ divides k.

Exercise 7. Find $\gcd(231, 163)$, as well as integers u, v such that

$$231u + 163v = \gcd(231, 163).$$

Exercise 8. The *Euler function* $\phi : \mathbf{N} \to \mathbf{N}$ is the function defined for every positive integer n by

$$\phi(n) = |\{k \in \{1, \dots, n\},\ k \text{ relatively prime to } n\}|.$$

1. What is the value of $\phi(p)$ for a prime number p ?
2. What is, in terms of k, the value of $\phi(p^k)$ where p is a prime number and $k \geq 1$ an integer?
3. Compute $\phi(n)$ for all integers n in the set $\{1, 2, \dots, 12\}$.

Exercise 9. Let n be an integer, and a, b non-zero relatively prime integers. Show that if both a and b divide n, then the product ab divides n. Does this remain true if a and b are no longer assumed to be relatively prime?