Margaret Bilu
Office 604 Fall 2019
bilu@cims.nyu.edu

Algebra homework 2
Arithmetic on the set of integers

Due September 25th, 2019

Please hand in your homework stapled, with your name written on it. All answers have to be justified.

Exercise 1. Prove the following properties:

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

Solution. Let $a, b, c \in \mathbf{Z}$. Let us suppose that $a|b$ and $b|c$. By definition, there exist $p, q \in \mathbf{Z}$ such that $b = pa$ and $c = qb$. Substituting b in the second equality, we get: $c = (qp) \times a$, with $qp \in \mathbf{Z}$.Therefore, $a \mid c$.

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

Solution. By definition, there exist $p, q \in \mathbf{Z}$ such that $b = pa$ and $a = qb$. Substituting b in the second equality, we get: $a = (qp) \times a$, which implies $qp = 1$, i.e. $p = q = 1$ or $p = q = -1$. Therefore $a = b$ or $a = -b$.

(c) If a, b, c are integers such that $a|b$ and $a|c$, then for all integers $u, v \in \mathbf{Z}$, a divides $ub + vc$.

Solution. By definition, there exist integers p, q such that $b = pa$ and $c = qa$. Then for all integers u, v,

$$ub + vc = upa + vqa = (up + vq)a,$$

which is divisible by a.

Exercise 2. Let p be a prime number. 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 $k \geq 1$.

*Solution.*The divisors of p^2 are $1, p, p^2$. The divisors of p^3 are $1, p, p^2, p^3$. More generally, for $k \geq 1$, the divisors of p^k are $1, p, p^2, \ldots, p^k$.

Exercise 3. For any integers a, b which are not both zero, prove the following properties of the greatest common divisor:

(a) For any non-zero integer k, $\gcd(ka, kb) = |k| \gcd(a, b)$.

Solution. First of all, note that $\gcd(-ka, -kb) = \gcd(ka, kb)$ (that is, the gcd does not depend on the sign). Thus, we may assume, without loss of generality, that $k > 0$.

Given this, we present three methods for proving the above identity.

First method: run the Euclidean algorithm for a and b, to get

$$\begin{array}{rcll} a &=& bq_0 + r_1, & 0 \le r_1 < b \\ b &=& r_1 q_1 + r_2, & 0 \le r_2 < r_1 \\ r_1 &=& r_2 q_2 + r_3, & 0 \le r_3 < r_2 \\ &\vdots&& \\ r_{n-2} &=& r_{n-1}q_{n-1} + r_n, & 0 \le r_n < r_{n-1} \\ r_{n-1} &=& r_n q_n. & \end{array}$$

Now multiply everything by k, to get:

$$\begin{array}{rcll} ka &=& (kb)q_0 + kr_1, & 0 \le kr_1 < kb \\ kb &=& (kr_1)q_1 + kr_2, & 0 \le kr_2 < kr_1 \\ kr_1 &=& (kr_2)q_2 + kr_3, & 0 \le kr_3 < kr_2 \\ &\vdots&& \\ kr_{n-2} &=& (kr_{n-1})q_{n-1} + kr_n, & 0 \le kr_n < k_{n-1} \\ kr_{n-1} &=& (kr_n)q_n. & \end{array}$$

We see that we still get a succession of Euclidean divisions (the remainders still satisfy the right bounds), so that this is the Euclidean algorithm for computing the gcd of ka and kb. Thus, $\gcd(ka, kb)$ is the last non-zero remainder, that is, $kr_n = k\gcd(a, b)$.

Second method: Find u and v such that $uka+vkb = \gcd(ka, kb)$. Since the left-hand side is divisible by k, we find that $\gcd(ka, kb)$ must be divisible by k. Moreover, if we divide by k, we get

$$ua + vb = \frac{\gcd(ka, kb)}{k}$$

Here the left-hand side is divisible by $\gcd(a, b)$, so we get that $\frac{\gcd(ka,kb)}{k}$ must be a multiple of $\gcd(a, b)$. Thus, we see that $\gcd(ka, kb) = k\gcd(a, b)m$ for some positive integer m. It remains to prove that $m = 1$. We have that $k\gcd(a, b)m$ divides both ka and kb. This means that $\gcd(a, b)m$ divides a and b, so it is a common divisor of a and b. But $\gcd(a, b)$ is the greatest common divisor of a and b, so we must have $m = 1$.

Third method: Starting like in the previous method, we see that $\gcd(ka, kb)$ must be divisible by k. Now, let d be a common divisor of ka and kb which is a multiple of k. We may write $d = kd'$. Since kd' divides ka and kb, we have that d' divides a and b. Thus, any common divisor of d which is a multiple of k is of the form kd' where d' is a common divisor of a and b. The largest integer of this form is $k\gcd(a, b)$, which is indeed a common divisor of ka and kb, so we have $\gcd(ka, kb) = k\gcd(a, b)$.

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

Solution. We know that d divides both a and b, so there exist integers a', b' such that $a = da'$ and $b = db'$. There are different ways for concluding that a' and b' are relatively prime:

- Either you use the previous question:

$$d = \gcd(da', db') = d \gcd(a', b')$$

  from which we conclude $\gcd(a', b') = 1$.
- Or you use the fact that there exist u and v such that $ua + vb = d$. Cancelling out d on both sides, we get $ua' + vb' = 1$, so by Bézout's theorem a' and b' are relatively prime.

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

Solution. Let d be a common divisor of a and b. Then d also divides $a + b$. Thus, d is also a common divisor of $a+b$ and b. Conversely, if d is a common divisor of $a+b$ and b, then d also divides $(a + b) - b = a$, so d is a common divisor of a and b. We have shown that the sets

$$\{\text{common divisors of } a \text{ and } b\}$$

and

$$\{\text{common divisors of } a + b \text{ and } b\}$$

are equal. Comparing their largest elements, we get $\gcd(a, b) = \gcd(a + b, b)$.

(d) $\gcd(a, a + 1) = 1$.

Solution. Put $d = \gcd(a, a+1)$. If d divides a and $a+1$, then d divides $(a+1)-a = 1$. Since $d > 0$, we must have $d = 1$.

Another way of saying this is to write

$$1 \times (a + 1) - 1 \times a = 1$$

and conclude by Bézout's theorem.

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

Solution. Put $d = \gcd(a, a+k$. If d divides a and $a+k$, then d divides $(a+k)-a = k$.

Exercise 4. 1. Compute $\gcd(201, 694)$.

Solution. We run the Euclidean algorithm:

$$\begin{aligned} 694 &= 3 \times 201 + 91 \\ 201 &= 2 \times 91 + 19 \\ 91 &= 4 \times 19 + 15 \\ 19 &= 1 \times 15 + 4 \\ 15 &= 3 \times 4 + 3 \\ 4 &= 1 \times 3 + 1 \end{aligned}$$

Thus, the gcd is 1.

2. Find integers u and v such that $694u + 201v = \gcd(201, 694)$.

   Solution. We run the extended Euclidean algorithm:

$$\begin{aligned}
1 &= 4 - 1 \times 3 \\
&= 4 - 1 \times (15 - 3 \times 4) \\
&= 4 \times 4 - 1 \times 15 \\
&= 4 \times (19 - 1 \times 15) - 1 \times 15 \\
&= 4 \times 19 - 5 \times 15 \\
&= 4 \times 19 - 5 \times (91 - 4 \times 19) \\
&= 24 \times 19 - 5 \times 91 \\
&= 24 \times (201 - 2 \times 91) - 5 \times 91 \\
&= 24 \times 201 - 53 \times 91 \\
&= 24 \times 201 - 53 \times (694 - 3 \times 201) \\
&= 183 \times 201 - 53 \times 694
\end{aligned}$$

   Thus, $u = -53$ and $v = 183$ is a possible solution.

Exercise 5. Recall that for a set A, we denote by $|A|$ the number of its elements. The *Euler function* $\phi : \mathbf{N} \to \mathbf{N}$ is the function defined for every positive integer n by

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

1. What is the value of $\phi(p)$ for a prime number p ?

   Solution. When p is prime, all of the elements in the set $\{1, \ldots, p\}$, except p itself, are relatively prime to p. Therefore: $\phi(p) = p - 1$.

2. Compute $\phi(n)$ for all integers n in the set $\{1, 2, \ldots, 12\}$.

   Solution. You should get: $\phi(1) = 1$, $\phi(2) = 1$, $\phi(3) = 2$, $\phi(4) = 2$, $\phi(5) = 4$, $\phi(6) = 2$, $\phi(7) = 6$, $\phi(8) = 4$, $\phi(9) = 6$, $\phi(10) = 4$, $\phi(11) = 10$, $\phi(12) = 4$. (Use the previous question for all prime numbers!).

Exercise 6.

1. 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. (Hint: Bézout's theorem)

   Solution. Write $n = ka$ and $n = lb$. By Bézout, there exist integers u, v such that $ua + vb = 1$. Multiplying both sides by n, we get

$$uan + vbn = n.$$

   Now substitute the first occurrence of n by lb, and the second occurrence by ka. Then we get

$$uk(ab) + vl(ab) = n.$$

   Thus, the left-hand side is divisible by ab, so n is divisible by ab.

2. Does this remain true if a and b are no longer assumed to be relatively prime?

   Solution. No, for example if $a = b = 2$, both a and b divide 2, but ab does not.