Math 261 — Exercise sheet 2

http://staff.aub.edu.lb/~nm116/teaching/2017/math261/index.html

Version: September 25, 2017

Answers are due for Monday 25 September, 11AM.

The use of calculators is allowed.

Exercise 2.1

Find **all** solutions $x, y \in \mathbb{Z}$ to the following equations:

1. $3x + 5y = 2$,
2. $18x + 30y = 2016$,
3. $18x + 30y = 2017$.

Solution 2.1

1. Since 3 and 5 are coprime, this equation has solutions. An obvious one is $x = -1$, $y = 1$, and we know that we get all the other ones by adding a multiple of 3×5 on one side, and compensating on the other side. So the solutions are exactly the

   $$x = -1 + 5t, \ y = 1 - 3t \quad (t \in \mathbb{Z}).$$

2. This time 18 and 30 are not coprime, but their gcd, which is 6, divides 2016, so we can get an equivalent equation by dividing everything by 6:

   $$3x + 5y = 336.$$

   We spot a solution, for instance $y = 60, x = 12$; and the other solutions differ by multiples of 3×5. So finally the solutions are

   $$x = 12 + 5t, \ y = 60 - 3t \quad (t \in \mathbb{Z}).$$

3. This time, $\gcd(18, 30) = 6$ does not divide 2017, so the equation has no solutions.

Exercise 2.2: The lcm

1. Let I and J be two ideals of $\mathbb{Z}$. Apply the definition of an ideal to prove that the intersection $I \cap J$ is also an ideal of $\mathbb{Z}$.

2. Let a and b be positive integers. By the previous question, $a\mathbb{Z} \cap b\mathbb{Z}$ is an ideal of $\mathbb{Z}$. Prove that this ideal is not the zero ideal. Why does this imply that there exists a positive integer c such that $a\mathbb{Z} \cap b\mathbb{Z} = c\mathbb{Z}$?

3. The integer c defined in the previous question is called the *lowest common multiple* of a and b, and is denoted by $\operatorname{lcm}(a, b)$. Explain this name.

4. Let $p_1, \cdots, p_n$ be the primes that divide either a or b, so that we may write
$$a = \prod_{i=1}^{n} p_i^{u_i}, \qquad b = \prod_{i=1}^{n} p_i^{v_i}$$
with non-negative integers $u_1, \cdots, u_n$ and $v_1, \cdots, v_n$. Express $\operatorname{lcm}(a, b)$ in terms of the p_i, the u_i and the v_i.

5. Deduce that $\gcd(a, b) \operatorname{lcm}(a, b) = ab$.

   Remark: This means that it is possible to compute the lcm by computing the gcd through the Euclidian algorithm. When a and b are large, this is much more efficient than computing the factorization of a and b.

Solution 2.2:

1. - We know that every ideal of $\mathbb{Z}$ contains at least 0. So $0 \in I$, and $0 \in J$, so that $0 \in I \cap J$; as a result, $I \cap J$ is not empty.
   - Let x and y be elements of $I \cap J$. Then since x and y are in I, $x + y$ is in I; similarly, since x and y are in J, $x + y$ is also in J. So $x + y \in I \cap J$.
   - Finally, let $n \in \mathbb{Z}$, and let $x \in I \cap J$. Then $nx \in I$, and $nx \in J$, so $nx \in I \cap J$.

   This shows that $I \cap J$ is an ideal of $\mathbb{Z}$.

2. We have $ab \in a\mathbb{Z} \cap b\mathbb{Z}$, so $a\mathbb{Z} \cap b\mathbb{Z} \neq \{0\}$. Since every ideal of $\mathbb{Z}$ is of the form $c\mathbb{Z}$ for some $c \in \mathbb{Z}$, and since $a\mathbb{Z} \cap b\mathbb{Z}$ is an ideal by the previous question, there exists $c \in \mathbb{Z}$ such that $a\mathbb{Z} \cap b\mathbb{Z} = c\mathbb{Z}$. But since $ab \in a\mathbb{Z} \cap b\mathbb{Z}$, we cannot have $c = 0$, and since $c\mathbb{Z} = (-c)\mathbb{Z}$, we may assume that $c > 0$.

3. Clearly, c is the smallest positive element of the ideal $c\mathbb{Z}$. But $c\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$ is the set of integers that are both a multiple of a and of b. The number c is thus the smallest such common multiple, whence this name.

4. The formula $a\mathbb{Z} \cap b\mathbb{Z} = c\mathbb{Z}$ says that the common multiples of a and b are precisely the multiples of c. Now $ab = \prod_{i=1}^{n} p_i^{u_i+v_i}$ is such a common multiple, so c divides it; therefore $c = \prod_{i=1}^{n} p_i^{w_i}$ for some integers $w_i \leqslant u_i + v_i$.

   In order for c to be a multiple both of a and b, we need w_i to be both $\geqslant u_i$ and $\geqslant v_i$ for each i. Then c will be the smallest common multiple precisely when $w_i = \max(u_i, v_i)$, so that
$$c = \prod_{i=1}^{n} p_i^{\max(u_i, v_i)}.$$

5. Recall that $\gcd(a,b) = \prod_{i=1}^n p_i^{\min(u_i,v_i)}$. Now, $\min(u,v) + \max(u,v) = u + v$ for all u and v, so that

$$\gcd(a,b)\,\mathrm{lcm}(a,b) = \prod_{i=1}^n p_i^{\min(u_i,v_i)+\max(u_i,v_i)} = \prod_{i=1}^n p_i^{u_i+v_i} = ab.$$

Exercise 2.3

1. Use the Euclidian algorithm to determine if 47 is invertible mod 111, and to find its inverse if it is.

2. Solve the equation $47x \equiv 5 \pmod{111}$ in $\mathbb{Z}/111\mathbb{Z}$.

Solution 2.3

1. We know that 47 is invertible mod 111 if and only if 47 and 111 are coprime. If they are, we need to look for u and $v \in \mathbb{Z}$ such that $47u + 111v = 1$; indeed, u will then be an inverse of $47 \pmod{111}$. To find u and v, we either spot them directly[1], or we use the Euclidian algorithm. This algorithm will also tell us if the gcd of 47 and 111 is not 1, so let's apply it:

$$\begin{aligned} 111 &= 2 \times 47 + 17 \\ 47 &= 2 \times 17 + 13 \\ 17 &= 13 + 4 \\ 13 &= 3 \times 4 + 1 \end{aligned}$$

So the gcd is 1, so 47 is invertible mod 111. To find it, we write

$$\begin{aligned} 1 &= 13 - 3 \times 4 \\ &= 13 - 3(17 - 13) = 4 \times 13 - 3 \times 17 \\ &= 4(47 - 2 \times 17) - 3 \times 17 = 4 \times 47 - 11 \times 17 \\ &= 4 \times 47 - 11 \times (111 - 2 \times 47) = 26 \times 47 - 11 \times 111, \end{aligned}$$

whence 26 mod 111 is the inverse of 47 mod 111.

2. Since 47 is invertible mod 111, the only solution is

$$x = 5 \times 47^{-1} = 5 \times 26 = 130 \equiv 19 \pmod{111}.$$

[1] It can happen sometimes, but here there are no obvious candidates

Exercise 2.4: An unsolvable diophantine equation

Prove that the equation $x^3 + y^3 + z^3 = 31$ has no solution with $x, y, z \in \mathbb{Z}$.

Hint: try solving the equation mod 9.

Solution 2.4:

Let us make a table of the cubes in $\mathbb{Z}/9\mathbb{Z}$:

x	-4	-3	-2	-1	0	1	2	3	4
x^3	-1	0	1	-1	0	1	-1	0	1

So the only cubes in $\mathbb{Z}/9\mathbb{Z}$ are -1,0 and 1. As a result, a sum of 3 cubes can be $-3, -2, -1, 0, 1, 2$ or 3 (mod 9), but it can never be 4 nor -4. Since $31 \equiv 4 \pmod 9$, the equation $x^3 + y^3 + z^3 = 31$ has no solution in $\mathbb{Z}/9\mathbb{Z}$; therefore, it has no solution in $\mathbb{Z}$ either.

Exercise 2.5: Primes mod 6

1. Let p be a prime number which is neither 2 nor 3. Prove that either $p \equiv 1 \pmod 6$ or $p \equiv -1 \pmod 6$.

2. Prove that there are infinitely many primes p such that $p \equiv -1 \pmod 6$.

   Hint: Suppose on the contrary that there are finitely many, say $p_1, \cdots, p_k$. Let $N = 6p_1 \cdots p_k - 1$, and consider a prime divisor of N.

3. Why does the same proof fail to show that there are infinitely may primes p such that $p \equiv 1 \pmod 6$?

4. *Dirichlet's theorem on primes in arithmetic progressions*, which is way beyond the scope of this course, states that for all coprime positive integers a and b, there are infinitely many primes p such that $p \equiv a \pmod b$; in particular, there are in fact infinitely many primes p such that $p \equiv 1 \pmod 6$. Why, in the statement of this theorem, is it necessary to assume that a and b are coprime ?

Solution 2.5:

1. If p is netiher 2 nor 3, then $p \nmid 6$, so p and 6 are coprime. But the only invertibles in $\mathbb{Z}/6\mathbb{Z}$ are ± 1 (either see it by inspection of all 6 elements, or use the fact that $\phi(6) = 2$), so we must have $p \equiv \pm 1 \pmod 6$.

2. Suppose that $p_1, \cdots, p_k$ are the only such primes, and let $N = 6p_1 \cdots p_k - 1$. Clearly, neither 2 nor 3 divide N (since $N \equiv -1 \bmod 6$), so the primes dividing N are all $\equiv \pm 1 \pmod 6$ by the previous question. If they were all $\equiv +1 \pmod 6$, then N, their product, would also be $\equiv +1 \pmod 6$, which is not the case. So at least one of them, say p, is $\equiv -1 \pmod 6$. But this p cannot be one of $p_1, \cdots, p_k$, else we would have $p \mid (6p_1 \cdots p_k - N) = 1$. We therefore have reached a contradiction.

3. We could suppose by contradiction that $p_1, \cdots, p_k$ are the only primes $\equiv 1 \pmod 6$, and consider a prime divisor of $N = 6p_1 \cdots p_k - 1$ (or $N = 6p_1 \cdots p_k + 1$). Such a prime could not be any of the p_i for the same reason as above, but there is no reason why it would have to be $\equiv 1 \pmod 6$; indeed, nothing prevents the divisors of N from being all $\equiv -1 \pmod 6$. So we are stuck.

4. If $p \equiv a \pmod{b}$, then $p = bx + a$ for some $x \in \mathbb{Z}$, so $\gcd(a,b) \mid p$; and obviously, if $\gcd(a,b) > 1$, this can only happen for at most one prime p (exactly one if $\gcd(a,b) = p$ is itself prime, and none else).

The exercise below has been added for practice. not mandatory. It is not mandatory, and not worth any points. The solution will be made available with the solutions to the other exercises.

Exercise 2.6: Divisibility criteria

Let $n \in \mathbb{N}$.

1. Prove that $3 \mid n$ iff. 3 divides the sum of digits of n.
2. Prove that $9 \mid n$ iff. 9 divides the sum of digits of n.
3. Find a similar criterion to test whether $11 \mid n$.

Solution 2.6:

The key is the following observation: if $n_0, n_1, n_2, \cdots$ are the digits of n from right to left, so that

$$n = n_0 + 10n_1 + 100n_2 + \cdots = \sum n_i 10^i,$$

and since $10 \equiv 1 \pmod{9}$, we have

$$n = \sum n_i 10^i \equiv \sum n_i 1^i = \sum n_i \pmod{9};$$

in other words, n is congruent to the sum of its digits (mod 9). In particular, this congruence also holds mod 3 since $3 \mid 9$.

So we have

$$9 \mid n \iff n \equiv 0 \pmod{9} \iff \sum n_i \equiv 0 \pmod{9} \iff 9 \mid \sum n_i$$

and

$$3 \mid n \iff n \equiv 0 \pmod{3} \iff \sum n_i \equiv 0 \pmod{3} \iff 3 \mid \sum n_i.$$

For divisibility by 11, we notice that $10 \equiv -1 \pmod{11}$, so that

$$n = \sum n_i 10^i \equiv \sum n_i (-1)^i = n_0 - n_1 + n_2 - n_3 + \cdots \pmod{11}.$$

As a result, $11|n$ if and only if the expression

$$n_0 - n_1 + n_2 - n_3 + \cdots ,$$

which is called the *alternate* sum of digits of n, is divisible by 11.

Examples:

- For $n = 261$, we have $2 + 6 + 1 = 9$, so $9 \mid 261$.
- For $n = 1452$, we have $2 - 5 + 4 - 1 = 0$, so $11 \mid 1452$.
- We also see that $11 \mid 261$ and that $3 \mid 1452$ but $9 \nmid 1452$.