Math 261 — Exercise sheet 2

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

Version: September 20, 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. $18x + 30y = 2017$.

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.

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 $\mathbb{Z}/111\mathbb{Z}$.

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.

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 ?

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 $11 \mid n$.