Math 261 — Exercise sheet 3

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

Version: October 1, 2018

Answers are due for Wednesday 03 October, 11AM.

The use of calculators is allowed.

Exercise 3.1: Divisibility by 11 (20 pts)

Prove that an integer is divisible by 11 if and only if the *alternate* sum of its digits is divisible by 11.
Here, alternate *means the sum is computed with alternating + and − signs. For instance,* 87406 *is divisible by* 11 *because* $8 - 7 + 4 - 0 + 6 = 11$ *is divisible by* 11.

Exercise 3.2: Not a sum of 2 squares (25 pts)

Let N be an integer. Prove that if $N \equiv -1 \bmod 4$, then N is not a sum of two squares (i.e. not of the form $x^2 + y^2$ with $x, y \in \mathbb{Z}$).

Exercise 3.3: An inverse (25 pts)

1. (15 pts) Use Euclid's algorithm to determine if 40 is invertible mod 111, and to find its inverse if it is.
2. (10 pts) Solve the equation $40x = 7$ in $\mathbb{Z}/111\mathbb{Z}$.

Exercise 3.4: Primes mod 4 (30 pts)

1. (5 pts) Let p be a prime number different from 2. Prove that $p \equiv \pm 1 \pmod 4$.

   Hint: What is $\gcd(p, 4)$*?*

2. (15 pts) Prove that there are infinitely many primes p such that $p \equiv -1 \pmod 4$.

   Hint: Suppose on the contrary that there are finitely many, say $p_1, \cdots, p_k$*. Let* $N = 4p_1 \cdots p_k - 1$*, and consider a prime divisor of* N*.*

3. (5 pts) Why does the same proof fail to show that there are infinitely may primes p such that $p \equiv 1 \pmod 4$?
4. (5 pts) *Dirichlet's theorem on primes in arithmetic progressions*, whose proof 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 $p \equiv 1 \pmod 4$. 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. It is not mandatory, and not worth any points. The solution will be made available with the solutions to the other exercises.

Exercise 3.5: More inverses (0 pt)

1. Fix $N \in \mathbb{N}$, and let $x \in (\mathbb{Z}/N\mathbb{Z})^\times$ be invertible, of inverse $y \in \mathbb{Z}/N\mathbb{Z}$. Prove that x^2, $-x$, and y are also invertible, and find their inverses.

2. Give all the elements of $(\mathbb{Z}/15\mathbb{Z})^\times$, and give the inverse of each of them. What is $\phi(15)$?

   Hint: Use the previous question to save your effort!