# Math 261 — Exercise sheet 3

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

Version: October 3, 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*.*

## Solution 3.1:

Let $n$ be our integer, and let $n_0, n_1, n_2, \cdots$ be its digits from right to left, so that

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

Since $10 \equiv -1 \pmod{11}$, we have

$$n = \sum n_i 10^i \equiv \sum n_i (-1)^i \pmod{11};$$

in other words, $n$ is congruent to plus or minus (depending on which sign the most significant digit takes in the sum) the alternate sum of its digits (mod 11). In particular, $n$ is 0 (mod 11) if and only if this sum is 0 (mod 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 $x, y \in \mathbb{Z}$).

## Solution 3.2:

The question encourages us to work in $\mathbb{Z}/4\mathbb{Z}$. Let us make a table of the squares in $\mathbb{Z}/4\mathbb{Z}$:

| $x$ | $-1$ | 0 | 1 | 2 |
|---|---|---|---|---|
| $x^2$ | 1 | 0 | 1 | 0 |

So the only squares in $\mathbb{Z}/4\mathbb{Z}$ are 0 and 1. As a result, a sum of two squares can be 0, 1 or 2 mod 4, but not $-1$.

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

## Solution 3.3:

1. We know that 40 is invertible mod 111 if and only if 40 and 111 are coprime. If they are, we need to look for $x$ and $y \in \mathbb{Z}$ such that $40x + 111y = 1$; indeed, $x$ will then be an inverse of 40 (mod 111). To find $x$ and $y$, we either spot them directly[1], or we use the Euclidian algorithm. This algorithm will also tell us if the gcd of 40 and 111 is not 1, so let's apply it:

$$\begin{aligned} 111 &= 2 \times 40 + 31 \\ 40 &= 1 \times 31 + 9 \\ 31 &= 3 \times 9 + 4 \\ 9 &= 2 \times 4 + 1 \end{aligned}$$

So the gcd is 1, so 40 is invertible mod 111. To find the inverse, we write

$$\begin{aligned} 1 &= 9 - 2 \times 4 \\ &= 9 - 2(31 - 3\times) = 7 \times 9 - 2 \times 31 \\ &= 7(40 - 31) - 2 \times 31 = 7 \times 40 - 9 \times 31 \\ &= 7 \times 40 - 9 \times (111 - 2 \times 40) = 25 \times 47 - 9 \times 111, \end{aligned}$$

whence $25 \in \mathbb{Z}/111\mathbb{Z}$ is the inverse of $40 \in \mathbb{Z}/111\mathbb{Z}$.

2. Since 40 is invertible mod 111, the only solution is

$$x = 7 \times 40^{-1} = 7 \times 25 = 175 = 64 \in \mathbb{Z}/111\mathbb{Z}.$$

## 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 $p \equiv 1 \pmod 4$?

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

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 ?

## Solution 3.4:

1. If $p \neq 2$ it is odd, so $p$ and 4 are coprime. But the only invertibles in $\mathbb{Z}/4\mathbb{Z}$ are $\pm 1$, so we must have $p \equiv \pm 1 \pmod{4}$.

2. Suppose that $p_1, \cdots, p_k$ are the only such primes, and let $N = 4p_1 \cdots p_k - 1$. Clearly, $N$ is odd, so the primes dividing $N$ are all $\equiv \pm 1 \pmod{4}$ by the previous question. If they were all $\equiv +1 \pmod{4}$, then $N$, their product, would also be $\equiv +1 \pmod{4}$, which is not the case. So at least one of them (and in fact, an odd number of them), say $p$, is $\equiv -1 \pmod{4}$. But this $p$ cannot be one of $p_1, \cdots, p_k$, else we would have $p \mid (4p_1 \cdots p_k - N) = 1$. We therefore have reached a contradiction.

3. We could suppose by contradiction that $p_1, \cdots, p_k$ are the only primes $\equiv 1 \pmod{4}$, and consider a prime divisor of $N = 4p_1 \cdots p_k - 1$ (or $N = 4p_1 \cdots p_k + 1$). 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 $\equiv 1 \pmod{4}$; indeed, nothing prevents the divisors of $N$ from being all $\equiv -1 \pmod{4}$. 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. 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!*

## Solution 3.5:

1. We are tempted to write

$$\frac{1}{x^2} = \left(\frac{1}{x}\right)^2 = y^2, \quad \frac{1}{-x} = -\frac{1}{x} = -y, \quad \frac{1}{y} = \frac{1}{1/x} = x,$$

   and to conclude that $x^2$, $-x$, aand $y$ are invertible, of respective inverses $y^2$, $-y$, and $x$. Let us check:

$$x^2y^2 = (xy)^2 = 1^2 = 1, \quad (-x)(-y) = xy = 1, \quad yx = xy = 1$$

   since $xy = 1$ as $y$ is the inverse of $x$. This proves that our intuition is correct.

2. The elments of $\mathbb{Z}/15\mathbb{Z}$ can be representated by $-7, -6, \cdots, 5, 6, 7$. Among these, the invertible ones are the ones that are coprime with 15, namely $-7, -4, -2, -1, 1, 2, 4, 7$. That's 8 of them, so $\phi(15) = 8$.

   Let us now match each element with its inverse, Obviously, 1 and $-1$ are ther own inverses. Also, the inverse of 2 is $8 = -7$ since $2 \cdot 8 = 16 = 1$ in $\mathbb{Z}/15\mathbb{Z}$. By the previous question, we immediately get that the inverses of 4, $-2$ and $-7$ are respectively $(-7)^2 = 49 = 4$, $- - 7 = 7$, and 2. It is now easy to complete the following table:

| $x$ | $-7$ | $-4$ | $-2$ | $-1$ | $1$ | $2$ | $4$ | $7$ |
|---|---|---|---|---|---|---|---|---|
| $x^{-1}$ | $2$ | $-4$ | $-1$ | $1$ | $-7$ | $4$ | $-2$ | |