Math 261 — Exercise sheet 5

http://staff.aub.edu.lb/~nm116/teaching/2018/math261/index.html

Version: October 24, 2018

Answers are due for Wednesday 24 October, 11AM.

The use of calculators is allowed.

Exercise 5.1: Some factorizations of polynomials mod p (100 pts)

Let $f(x)$ be the polynomial $x^3 - 8x^2 + 19x + 1$. Factor $f(x)$

1. (25 pts) mod 2,
2. (25 pts) mod 3,
3. (25 pts) mod 7,
4. (25 pts) mod 13.

Make sure that your factorizations are complete, i.e. prove that the factors that you find are irreducible.

Solution 5.1:

A polynomial of degree 3 is either irreducible, or splits as degree 2 × degree 1, or into 3 factors of degree 1 (not necessarily distinct). As a result, we can always factor it if we know what its roots are.

1. We have $f(x) \equiv x^3 + x + 1 \pmod 2$. Let us make a table of values in $\mathbb{Z}/2\mathbb{Z}$:

x	0	1
$f(x)$	1	1

   We see that $f(x)$ has no root in $\mathbb{Z}/2\mathbb{Z}$. Therefore, it is irreducible, so the complete factorization is

   $$f(x) \equiv x^3 + x + 1 \pmod 2.$$

2. We have $f(x) \equiv x^3 + x^2 + x + 1 \pmod 3$. Table of values of $f(x)$ mod 3:

x	0	1	-1
$f(x)$	1	1	0

   so $f(x)$ has one root in $\mathbb{Z}/3\mathbb{Z}$, namely -1.

   $$f(x) \equiv (x+1)g(x) \pmod 3,$$

where $g(x)$ has degree 2, so is either irreducible or a product of two factors of degree 1. We compute that $g(x) = x^2 + 1$; since any root of g is also a root of f, the only possible root of g is $x = -11$. But this is not a root of g, so g is irreducible, and the complete factorisation of f mod 5 is

$$f(x) \equiv (x+1)(x^2+1) \pmod 3.$$

3. Table of values of $f(x)$ mod 7:

x	0	1	2	3	-3	-2	-1
$f(x)$	1	-1	1	-1	-1	0	1

so -2 is the only root of $f(x)$ in $\mathbb{Z}/7\mathbb{Z}$.

As a result, we have

$$f(x) \equiv (x+2)g(x) \pmod 7$$

with $g(x)$ of degree 2, whose only possible root is -2. So either $g(x) = (x+2)^2$ (since the coefficient of x^3 in $f(x)$ is 1), or $g(x)$ is irreducible.

To figure out which, we can simply compute $g(x)$ by dividing $f(x)$ by $(x+2)$, and test whether -2 is a root of $g(x)$. We could also divide $f(x)$ by $(x+2)^2$, since if the remainder is 0 this will tell us that $(x+2) \mid g(x)$; however if it is not 0 we will know that $g(x)$ is irreducible, but we won't know which polynomial it is exactly, so this approach may fail. We could also simply test whether $f(x) \equiv (x+2)^3 \pmod 7$, but again, if this is not the case, we will know that $g(x)$ is irreducible, but not who it is.

So the safe way is to divide $f(x)$ by $(x+2)$. We find that $g(x) = x^2+4x+4 = (x+2)^2$, and $x = -2$ is a root of it! So

$$f(x) \equiv (x+2)^3 \pmod 7.$$

4. When we start to compute a table of values of $f(x)$ mod 13, we get this:

x	0	1	2	3	4	$\cdots$
$f(x)$	1	0	2	0	0	$\cdots$

At this point, we can stop: since f has 3 distinct roots and is of degree 3, it must split into

$$f(x) \equiv (x-1)(x-3)(x-4) \pmod{13}.$$

Remark 1: it is true that if $x = a$ is a root of $f(x)$, then $f(x)$ is divisible by $(x-a)^2$ iff. $x = a$ is also a root of the derivative $f'(x)$, but we did not see it in class (not enough time). In this exercise, this fact makes the computations much easier for $p = 3$ and $p = 7$.

Remark 2: If $f(x)$ were reducible in $\mathbb{Z}[x]$, then its factorization in $\mathbb{Z}[x]$ would survive mod p for every p. Therefore, the fact that there exists a p (namely, $p = 2$) such that $f(x)$ is irreducible mod p proves that $f(x)$ is irreducible over $\mathbb{Z}$.

The exercises below are not mandatory. They are not worth any points, and are given here for you to practise. The solutions will be made available with the solutions to the other exercises.

Exercise 5.2: More factorizations

Let $f(x)$ be the polynomial $x^3 - 3x^2 - 1$. Factor $f(x)$

1. mod 2,
2. mod 3,
3. mod 5,
4. mod 7.

Make sure that your factorizations are complete, i.e. prove that the factors that you find are irreducible.

Solution 5.2:

A polynomial of degree 3 is either irreducible, or splits as degree 2 $\times$ degree 1, or into 3 factors of degree 1 (not necessarily distinct). As a result, we can always factor it if we know what its roots are.

1. We have $f(x) \equiv x^3 + x^2 + 1 \pmod 2$. Let us make a table of values in $\mathbb{Z}/2\mathbb{Z}$:

x	0	1
$f(x)$	1	1

   We see that $f(x)$ has no root in $\mathbb{Z}/2\mathbb{Z}$. Therefore, it is irreducible, so the complete factorization is

   $$f(x) \equiv x^3 + x + 1 \pmod 2.$$

2. We have $f(x) \equiv x^3 - 1 \pmod 3$. Table of values:

x	0	1	2
$f(x)$	2	0	1

   so the only root of $f(x)$ in $\mathbb{Z}/3\mathbb{Z}$ is 1 (alternative reasoning: by Fermat's little theorem, we have $f(x) \equiv x - 1 \pmod 3$ for all $x \in \mathbb{Z}$). So $f(x)$ factors as $(x-1)g(x)$ mod 3, where $g(x)$ has degree 2. By Euclidian division over $\mathbb{Z}/3\mathbb{Z}$, we find that $g(x) = x^2 + x + 1$ (alternative proof: use the identity $x^3 - 1 = (x-1)(x^2 + x + 1)$, which is valid even over $\mathbb{Z}$ (as opposed to mod 3)). Since the only root of $f(x)$ in $\mathbb{Z}/3\mathbb{Z}$ is $x = 1$, the only possible root of $g(x)$ is also $x = 1$; and indeed $g(1) = 0$. So now we know that $x^3 - 1 = (x-1)^2 h(x)$, where $h(x)$ has degree 1. Since its only possible root is 1,and since the coefficient of x^3 in $x^3 - 1$ is 1, we must have $h(x) = x - 1$. As a conclusion, the complete factorization is

   $$f(x) \equiv (x-1)^3 \pmod 3.$$

   We could also have seen this directly, by writing

   $$x^3 - 1 = x^3 + (-1)^3 \equiv (x-1)^3 \pmod 3$$

   since we are in characteristic 3.

3. Table of values of $f(x)$ mod 5:

x	0	1	2	3	4
$f(x)$	4	2	0	4	0

so $f(x)$ has two roots in $\mathbb{Z}/5\mathbb{Z}$, namely 2 and 4. As a result, we have a factorization of the form

$$f(x) \equiv (x-2)(x-4)g(x) \pmod 5,$$

where $g(x)$ has degree 1. Since the only roots of $f(x)$ are 2 and 4, and since the coefficient of x^3 in $f(x)$ is 1, we have either $g(x) = x-2$ or $g(x) = x-4$.

There are two ways to discover which: compute $g(x)$ by dividing $f(x)$ by $(x-2)(x-4) = x^2 - x - 2$ over $\mathbb{Z}/5\mathbb{Z}$, or divide $f(x)$ by $(x-2)^2$; indeed, if we get remainder 0, we will know that $(x-2)^2$ divides $f(x)$, so the missing factor $g(x)$ must be $x-2$, else the missing factor is not $x-2$ so by elimination is must be $x-4$ (we could of course divide by $(x-4)^2$ instead of $(x-2)^2$ and apply the same reasoning).

Either way, we find that $g(x) = x-2$, so that the complete factorization is

$$f(x) \equiv (x-2)^2(x-4) \pmod 5.$$

4. Table of values of $f(x)$ mod 7:

x	0	1	2	3	4	5	6
$f(x)$	6	4	2	6	1	0	2

so 5 is the only root of $f(x)$ in $\mathbb{Z}/7\mathbb{Z}$.

As a result, we have

$$f(x) \equiv (x-5)g(x) \pmod 7$$

with $g(x)$ of degree 2, whose only possible root is 5. So either $g(x) = (x-5)^2$ (since the coefficient of x^3 in $f(x)$ is 1), or $g(x)$ is irreducible.

To figure out which, we can simply compute $g(x)$ by dividing $f(x)$ by $(x-5)$, and test whether 5 is a root of $g(x)$. We could also divide $f(x)$ by $(x-5)^2$, since if the remainder is 0 this will tell us that $(x-5) \mid g(x)$; however if it is not 0 we will know that $g(x)$ is irreducible, but we won't know which polynomial it is exactly, so this approach may fail. We could also simply test whether $f(x) \equiv (x-5)^3 \pmod 7$, but again, if this is not the case, we will know that $g(x)$ is irreducible, but not who it is.

So the safe way is to divide $f(x)$ by $(x-5)$. We find that $g(x) = x^2 + 2x + 3$, and $x = 5$ is not a root of it, so $g(x)$ must be irreducible, and so the complete factorization is

$$f(x) \equiv (x-5)(x^2+2x+3) \pmod 7.$$

Remark 1: it is true that if $x = a$ is a root of $f(x)$, then $f(x)$ is divisible by $(x-a)^2$ iff. $x = a$ is also a root of the derivative $f'(x)$, but we did not see it in class

(not enough time). In this exercise, this fact makes the computations much easier for $p = 3$ and $p = 5$.

Remark 2: If $f(x)$ were reducible in $\mathbb{Z}[x]$, then its factorization in $\mathbb{Z}[x]$ would survive mod p for every p. Therefore, the fact that there exists a p (namely, $p = 2$) such that $f(x)$ is irreducible mod p proves that $f(x)$ is irreducible over $\mathbb{Z}$.

Exercise 5.3: Irreducible polynomials over $\mathbb{Z}/2\mathbb{Z}$

1. Find all irreducible polynomials of degree 2 over $\mathbb{Z}/2\mathbb{Z}$.

2. Use the previous question and a Euclidean division to deduce that the polynomial $x^4 + x + 1$ is irreducible over $\mathbb{Z}/2\mathbb{Z}$.

Solution 5.3:

1. A polynomial of degree 2 is irreducible if and only if it has no roots (this is a general fact and has nothing to with $\mathbb{Z}/2\mathbb{Z}$; this is just saying that a polynomial of degree 2 is either irreducible or factors as a product of two polynomials of degree 1). So let $ax^2 + bx + c$ be a polynomial of degree 2, with $a, b, c \in \mathbb{Z}/2\mathbb{Z}$. We need $a \neq 0$ (else it's not of degree 2), and since $\mathbb{Z}/2\mathbb{Z} = \{0, 1\}$, we must have $a = 1$. We need our polynomial not to vanish at $x = 0$, so $c \neq 0$ so $c = 1$, and neither at $x = 1$, so $1 + b + 1 = b \neq 0$, so $b = 1$. We have thus proved that there is exactly one irreducible polynomial of degree 2:

$$x^2 + x + 1.$$

2. Let $f(x) = x^4 + x + 1$. We have $f(0) = f(1) = 1 \neq 0$, so this polynomial has no roots; since it has degree 4, it is thus either irreducible, or a product of two irreducible polynomials of degree 2 (any other factorization pattern would include at least one factor of degree 1, which would yield a root). We saw in the previous question that there is only one irreducible polynomial of degree 2, namely $g(x) = x^2 + x + 1$. So let us see if $f(x)$ is divisible by $g(x)$, by performing the Euclidian division of f by g. We find quotient $= x^2 + x$ and remainder $= 1$. Since the remainder is not zero, g does not divide f. So f must be irreducible.

   Remark: There was another way to show that. Indeed, if f had been a product of two irreducibles of degree 2, then since these irreducibles could only be g, and we would necessarily have had

$$f = g^2 = (x^2 + x + 1)^2 = x^4 + x^2 + 1.$$

   This is not the case, so f is irreducible.