Math 261 — Exercise sheet 3

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

Version: September 25, 2017

Answers are due for Monday 02 October, 11AM.

The use of calculators is allowed.

Exercise 3.1: Factorization of polynomials mod p (40 pts)

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

1. (10 pts) mod 2,
2. (10 pts) mod 3,
3. (10 pts) mod 5,
4. (10 pts) mod 7.

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

Solution 3.1:

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 3.2: (20 pts)

Find an integer x such that $x \equiv 12 \pmod 7$ and $x \equiv 7 \pmod{12}$.

Solution 3.2:

This is Chinese remainders: as 12 and 7 are coprime, we have a 1:1 correspondence

$$\mathbb{Z}/84\mathbb{Z} \longleftrightarrow \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}, \tag{$\star$}$$

and we are looking for a pre-image of $(12 \bmod 7, 7 \bmod 12)$ under this correspondence.

Let us start by finding u and v such that $7u + 12v = 1$. Either we spot them rightaway, or we use the Euclidian algorithm:

$$\begin{aligned} 12 &= 7+5 \\ 7 &= 5+2 \\ 5 &= 2\times 2+1 \end{aligned}$$

whence

$$1 = 5-2\times 2 = 5-2\times(7-5) = 3\times 5-2\times 7 = 3(12-7)-2\times 7 = 3\times 12-5\times 7.$$

So, under the correspondence $(\star)$, $3\times 12 = 36$ is a preimage of $(1 \bmod 7, 0 \bmod 12)$, and $-5\times 7 = -35$ is a preimage of $(0 \bmod 7, 1 \bmod 12)$. As a result, since

$$\begin{aligned} (12 \bmod 7, 7 \bmod 12) &= (5 \bmod 7, 7 \bmod 12) \\ &= 5\times(1 \bmod 7, 0 \bmod 12) + 7\times(0 \bmod 7, 1 \bmod 12), \end{aligned}$$

a preimage for $(12 \bmod 7, 7 \bmod 12)$ is $x = 5\times 36 + 7\times -35 = -65$.

Remark: Of course, any integer congruent to $-65 \pmod{84}$ *works (for instance, 19). In fact, the Chinese remainder theorem tells us that the solutions are exactly the numbers that are congruent to* $-65 \pmod{84}$*; no more, no less.*

Exercise 3.3: (10 pts)

Compute $\phi(261)$ and $\phi(6000)$.

Solution 3.3:

Thanks to the (complete) factorizations $261 = 3^2 \times 29$ and $6000 = 2^4 \times 3 \times 5^3$ and to the formula

$$\phi(n) = N \prod_{\substack{p|n \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right),$$

we find that

$$\phi(261) = 261(1 - 1/3)(1 - 1/29) = 3^2 \times 29 \times \frac{2}{3} \times \frac{28}{29} = 3 \times 2 \times 28 = 168$$

and that

$$\phi(6000) = 2^4 \times 3 \times 5^3 \times \frac{1}{2} \times \frac{2}{3} \times \frac{4}{5} = 2^3 \times 2 \times 5^2 \times 4 = 1600.$$

Exercise 3.4: $\phi(n)$ is always even (30 pts)

Prove that $\phi(n)$ is even for all $n \geqslant 3$.

Solution 3.4:

Let $n = \prod_i p_i^{a_i}$ be the factorization of n, where the p_i are distinct primes. Since ϕ is multiplicative, we have

$$\phi(n) = \prod_i \phi(p_i^{a_i}) = \prod_i p_i^{a_i - 1}(p_i - 1).$$

If n is not a power of 2, then one of the p_i is odd, so the term $(p_i - 1)$ is even and $\phi(n)$ is even.

If $n = 2^a$ is a power of 2, then we have $a \geqslant 2$ since $n \geqslant 3$, and so $\phi(n) = 2^{a-1}$ is also even.