Prof. Friedrich Eisenbrand
Nicolai Hähnle

Discussions from: April 19, 2011

Computer Algebra

Spring 2011

Assignment Sheet 5

Warning: These are just notes and not necessarily full solutions for each exercise. Full solutions may require some additional details to be fleshed out. Please report any mistakes you may find.

Exercise 1 (⋆)

By the Chinese Remainder Theorem, $\mathbb{Z}_{21} \cong \mathbb{Z}_3 \times \mathbb{Z}_7$. Let us determine the order of the elements of $\mathbb{Z}_3$ first. This is easy, because obviously the only invertible ones are 1 and $-1 \equiv 2$.

	0	1	2
ord	×	1	2

The × indicates that 0 is not invertible. For $\mathbb{Z}_7$, we know $|\mathbb{Z}_7^\star| = 6$. The order of each element must divide the size of the group, and so the only possible orders are 1, 2, 3, and 6. Since the group is cyclic, we can also immediately say that there is exactly one element with order 1 and 2 each (those elements are 1 and $-1 \equiv 6$, respectively), and two elements of order 3 and 6 each. With this knowledge, we compute

$$2^3 \equiv 1 \pmod 7$$

to determine $\mathrm{ord}(2) = 3$ and

$$3^3 \equiv 27 \equiv 6 \equiv -1 \pmod 7$$

to determine $\mathrm{ord}(3) \neq 3$, which implies $\mathrm{ord}(3) = 6$. Furthermore, we can immediately say, without computation, that

$$5^3 \equiv (-2)^3 \equiv -1 \pmod 7$$

so that $\mathrm{ord}(5) = 6$. And then $\mathrm{ord}(4) = 3$ follows, so we get

	0	1	2	3	4	5	6
ord	×	1	3	6	3	6	2

Now we can compute the orders of elements modulo 21, because $\mathbb{Z}_{21}^\star \cong \mathbb{Z}_3^\star \times \mathbb{Z}_7^\star$, and whenever we have a direct sum or product of abelian groups $G \oplus H$, then for $(g,h) \in G \oplus H$ one has $\mathrm{ord}((g,h)) = \mathrm{lcm}(\mathrm{ord}(g), \mathrm{ord}(h))$, where lcm is the least common multiple.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
ord_3	×	1	2	×	1	2	×	1	2	×	1	2	×	1	2	×	1	2	×	1	2
ord_7	×	1	3	6	3	6	2	×	1	3	6	3	6	2	×	1	3	6	3	6	2
ord_{21}	×	1	6	×	3	6	×	×	2	×	6	6	×	2	×	×	3	6	×	6	2

Again, the × marks elements that are non-invertible. Note, again, that elements are invertible if and only if they are coprime to 21. Furthermore, an element is a zero divisor if and

only if it is not invertible, for this specific ring.[1] In any ring, invertible elements $r \in R^\star$ are not zero divisors, for

$$rx = 0$$

implies $x = r^{-1}0 = 0$. In this specific ring, any non-invertible element shares a factor with 21, so multiplying it with the *other* factor results in a multiple of 21, which is congruent to 0, so any non-invertible element is a zero divisor. One can easily see that this equivalence is true of any ring of the form $\mathbb{Z}_N$, but it is false for many other rings, such as the integers $\mathbb{Z}$ or polynomial rings $k[x]$. The polynomial $x \in k[x]$ is not invertible, but it is also not a zero divisor. The same is true for $3 \in \mathbb{Z}$.

Finally, by exercise 3 we know that any primitive root of $\mathbb{Z}_{21}$ must have the same order in both $\mathbb{Z}_3$ and in $\mathbb{Z}_7$. From the table above, we see that the only candidates are 1 and $-1 \equiv 20$, both of which are easily verified to be primitive roots (of order 1 and 2, respectively).

Exercise 3

Let R and S be commutative rings and consider their product ring $T = R \times S$. Let $\omega = (\omega_R, \omega_S) \in T$. Prove that ω is a primitive n-th root of unity if and only if ω_R and ω_S are primitive n-th roots of unity in R and S, respectively.

Let us prove the statement from right to left first, so let ω_R and ω_S be primitive n-th roots of unity in R and S, respectively. Our goal is to show that $\omega := (\omega_R, \omega_S)$ is a primitive n-th root of unity in $R \times S$. By definition of multiplication and the multiplicative unit in a product ring:

$$\omega^n = (\omega_R, \omega_S)^n = (\omega_R^n, \omega_S^n) = (1_R, 1_S) = 1$$

Since $n \in R^\star$, there exists an inverse $n_R^{-1} \in R^\star$, similarly one has $n_S^{-1} \in S^\star$.[2]

$$n_T = (n_R, n_S)$$

and therefore

$$n_T \cdot (n_R^{-1}, n_S^{-1}) = (n_R, n_S) \cdot (n_R^{-1}, n_S^{-1}) = (n_R \cdot n_R^{-1}, n_S \cdot n_S^{-1}) = (1_R, 1_S) = 1,$$

which shows that n has an inverse in T, and so $n \in T^\star$. Finally, let $t|n$, $t \neq n$, and let $x = (x_R, x_S) \in T$ such that $(\omega^t - 1) \cdot x = 0$.

$$\begin{aligned}(0_R, 0_S) = 0 &= (\omega^t - 1) \cdot x \\ &= ((\omega_R, \omega_S)^t - (1_R, 1_S)) \cdot (x_R, x_S) \\ &= ((\omega_R^t - 1_R) \cdot x_R, (\omega_S^t - 1_S) \cdot x_S)\end{aligned}$$

We can separate this equality of pairs into two separate equalities:

$$\begin{aligned}0_R &= (\omega_R^t - 1_R) \cdot x_R \\ 0_S &= (\omega_S^t - 1_S) \cdot x_S\end{aligned}$$

[1] Assuming that we consider 0 as a zero divisor.

[2] When we talk of a natural number n in an arbitrary ring R, the underlying formal definition is the n-fold sum of the multiplicative unit, i.e. $n_R = 1_R + \cdots + 1_R$. Another way to look at this is via the natural ring homomorphism $\eta : \mathbb{Z} \to R$ defined by the natural extension of $\eta(1) := 1_R$.

Since $\omega_R^t - 1$ and $\omega_S^t - 1$ are not zero divisors, we can conclude that $x_R = 0$ and $x_S = 0$, i.e. $x = 0$. So we have shown that whenever $(\omega^t - 1) \cdot x = 0$, this implies that $x = 0$. In other words, $\omega^t - 1$ is not a zero divisor. This finishes the proof that ω is a primitive n-th root of unity.

Let us prove the other direction. Let $\omega = (\omega_R, \omega_S)$ be a primitive n-th root of unity. Showing $\omega_R^n = 1$ and ω_S^n, and $n \in R^\star$ and $n \in S^\star$ can be done by simply reversing the corresponding arguments above. Let $t|n$, $t \neq n$. We need to show that $\omega_R^t - 1$ is not a zero divisor. So let $x \in R$ such that $(\omega_R^t - 1) \cdot x = 0$.

$$(\omega^t - 1) \cdot (x, 0) = ((\omega_R^t - 1) \cdot x, (\omega_S^t - 1) \cdot 0) = (0, 0) = 0$$

Since $\omega^t - 1$ is not a zero divisor, this implies that $(x, 0) = 0$, which implies that $x = 0$. So whenever $(\omega_R^t - 1) \cdot x = 0$, this implies that $x = 0$. In other words, $\omega_R^t - 1$ is not a zero divisor. This completes the proof that ω_R is a primitive n-th root of unity, and of course the proof for ω_S is analogous.

Exercise 4 ($\star$)
Let R be a commutative ring and $\omega \in R$ such that $\omega^n = 1$ and $n \in R^\star$. Prove that the following are equivalent:

1. for all $k \in \mathbb{Z}$ such that n does not divide k, $(\omega^k - 1) \in R$ is not a zero divisor.
2. for all divisors t of n, $t \neq n$, the element $(\omega^t - 1) \in R$ is not a zero divisor.

The implication 1. $\implies$ 2. is easy, so let us only look at 2. $\implies$ 1. Let k be as given in 1., and let $t = \gcd(k, n)$. Note that $t|n$ and $t \neq n$. There exist integers x and y such that

$$t = kx + ny.$$

In fact, it is easy to see that we can assume $x > 0$.[3]

$$(\omega^k - 1)(1 + \omega^k + \omega^{2k} + \cdots + \omega^{(x-1)k}) = \omega^{kx} - 1 = \omega^{t-ny} - 1 = \omega^t - 1$$

It is a fact that any factor of a not-zero-divisor is itself a not-zero-divisor, which completes the proof because $\omega^t - 1$ is not a zero divisor according to 2.

To see the fact in this special case: suppose $r \in R$ is such that $(\omega^k - 1)r = 0$. Then multiplying both sides with $(1 + \omega^k + \cdots + \omega^{(k-1)x})$ results in $(\omega^t - 1)r = 0$, which shows that $r = 0$ because $\omega^t - 1$ is not a zero divisor. Since this is true for all $r \in R$, it implies that $\omega^k - 1$ is not a zero divisor.

Exercise 5
Let R be a ring with a primitive n-th root of unity $\omega \in R$. Prove:

1. ω^{-1} is a primitve n-th root of unity.

[3] Adding n to x while simultaneously subtracting k from y does not change the right hand side in $t = kx + ny$. This operation can be repeated until x is positive.

2. If n is even, then ω^2 is a primitive $(n/2)$-th root of unity. If n is odd, then ω^2 is a primitive n-th root of unity.

3. Let $k \in \mathbb{Z}$ and $d = n/\gcd(n,k)$. Then ω^k is a d-th root of unity.

It is easy to see that the first two points are special cases of the last point. So let $k \in \mathbb{Z}$ and $d = n/\gcd(n,k)$ and set $\nu := \omega^k$. Since $k/\gcd(n,k)$ is integral, we can compute

$$\nu^d = \omega^{kd} = \omega^{kn/\gcd(n,k)} = (\omega^n)^{k/\gcd(n,k)} = 1.$$

Since d is a factor of n, it follows that $d \in R^\star$. In particular, $n^{-1} \cdot \gcd(n,k)$ is an inverse of d in R.

Now let $t|d$, $t \neq d$. It remains to prove that $\nu^t - 1$ is not a zero divisor.

$$\nu^t - 1 = \omega^{kt} - 1$$

If we can show that n does not divide kt, then we are done by the previous exercise.

So assume that $n|kt$. Then $d \cdot \gcd(n,k)|kt$ and, since $\gcd(n,k)|k$, $d|\frac{k}{\gcd(n,k)}t$. Now observe that d and $k/\gcd(n,k)$ are coprime (otherwise, their common factor would contribute to $\gcd(n,k)$). It follows that $d|t$, which contradicts the conditions on t. This completes the proof that $\nu^t - 1$ is not a zero divisor, and so all properties of a primitive d-th root of unity are satisfied.

Exercise 6

What is the number of primitive n-th roots of unity in $\mathbb{C}$?

Since $\mathbb{C}$ is a field of characteristic zero, one has $n \in \mathbb{C}^\star$ and there is no zero divisor except zero itself. So the conditions for primitive roots can be reduced to: $\omega^n = 1$ and $\omega^k \neq 1$ for $1 \leq k < n$. Let us define

$$C_n := \{z \in \mathbb{C} \mid z^n = 1\}$$

It is easy to see that C_n consists of n points on the unit circle of the complex plane, and that C_n is a cyclic subgroup of $\mathbb{C}^\star$ (under multiplication) with neutral element 1. Furthermore, using the above conditions for primitive roots, it is clear that z is a primitive n-th root of unity if and only if $z \in C_n$ is a group element of order n.

So the question is reduced to the following: in a cyclic group of n elements, how many elements have order n?

To answer this question, we use the fact that $C_n \cong \mathbb{Z}/n\mathbb{Z}$, the group of numbers modulo n under addition. If an element $x \in \mathbb{Z}/n\mathbb{Z}$ is of order less than n, then by definition there exists $1 \leq a < n$ such that $a \cdot x \equiv 0 \pmod{n}$.[4] Written explicitly, one has $n|ax$. Since a is not a multiple of n, this implies that $\gcd(x,n) \neq 1$.

Conversely, if $\gcd(x,n) \neq 1$, then $\frac{n}{\gcd(x,n)} \cdot x \equiv 0 \pmod{n}$. That is, the order of x in $\mathbb{Z}/n\mathbb{Z}$ is strictly less than n.

[4] Remember that the group operation in $\mathbb{Z}/n\mathbb{Z}$ is addition. Therefore, taking x to the a-th power *in this group* is actually a-fold addition, which is the same as integer multiplication by a. Furthermore, the neutral element with respect to addition is 0, not 1.

To summarize, an element x is of order less than n if and only if $\gcd(x,n) \neq 1$. The contrapositive of this is: an element x is of order n if and only if $\gcd(x,n) = 1$.[5] The number of such elements is given by the Euler φ function. It follows that the number of primitive n-th roots of unity in $\mathbb{C}$ is $\varphi(n)$.

Exercise 7

Let $n \in \mathbb{N}$. Show that 2 is a primitive $2n$-th root of unity modulo 2^n+1 if and only if n is a power of 2.

Let us first show the "if" part. Let n be a power of 2.

$$2^{2n} \equiv (2^n)^2 \equiv (-1)^2 \equiv 1 \pmod{2^n+1}$$

Furthermore, $\gcd(2n, 2^n+1) = 1$ because $2n$ is a power of two, whereas $2^n+1 \equiv 1 \pmod 2$. So we have $2n \in (\mathbb{Z}/(2^n+1)\mathbb{Z})^\star$.

Now let $t|2n$, $t \neq 2n$. We need to show that 2^t-1 is not a zero divisor.

Let us first handle the case $t = n$.

$$2^n - 1 \equiv -2 \pmod{2^n+1}$$

Since $\gcd(-2, 2^n+1) = 1$ similarly to the argument above, we know that 2^n-1 is invertible and therefore not a zero divisor.

Now suppose that $t \neq n$, which implies that $n = tk$ for some k because $2n$ is a power of two.

$$(2^t-1)(1+2^t+\cdots+2^{(k-1)t}) = 2^{kt}-1 = 2^n-1$$

So 2^t-1 is a factor of a 2^n-1. Combined with the fact that 2^n-1 is not a zero divisor, this implies that 2^t-1 is not a zero divisor.[6] Thus the proof that 2 is a primitive $2n$-th root of unity modulo 2^n+1 is completed.

Let us now turn to the "only if" part. Suppose that n is not a power of two, that is, n has an odd prime factor p.

Assume that 2 is a primitive $2n$-th root of unity modulo 2^n+1. Then by exercise 5, $\omega := 2^{2n/p}$ is a primitive p-th root of unity. One of the fundamental facts about primitive roots of unity tells us that we have[7]

$$1+\omega+\cdots+\omega^{p-1} \equiv 0 \pmod{2^n+1}. \tag{1}$$

We want to derive a contradiction from this equation. Observe that the powers of 2 modulo 2^n+1 can be divided into "positive" and "negative" numbers.

k	0	1	2	3	…	$n-1$	n	$n+1$	$n+2$	…	$2n-1$
2^k	1	2	4	8	…	2^{n-1}	-1	-2	-4	…	-2^{n-1}

[5] Here we implicitly use the fact that the order of a group element divides the number of elements of the group, so that the order of an element is either n or less than n.

[6] This is analogous to the argument in exercise 4. In fact, since we showed that 2^n-1 is invertible, this even implies that 2^t-1 is invertible, which is no surprise. Recall the observation in exercise 1 that zero divisor and non-invertible are the same thing in rings of the form $\mathbb{Z}/m\mathbb{Z}$.

[7] This is because $(\omega-1)(1+\omega+\cdots+\omega^{p-1}) \equiv \omega^p - 1 \equiv 0$ and $\omega-1$ is not a zero divisor. Furthermore, this is the reason for our interest in primitive roots in the first place, because it allows the discrete Fourier transform to work.

It goes without saying that those numbers are not "positive" or "negative" in the usual sense, since the usual notion simply does not make sense in modular arithmetic. When we say that the powers 2^k with $0 \le k \le n-1$ are positive and the powers with $n \le k \le 2n-1$ are negative, then these are new definitions of the words "positive" and "negative" that are only superficially related to the usual definitions.

Since no summand appears multiple times in (1), we can separate the summands into a set S_+ of positive and a set S_- of negative summands in such a way that

$$\sum_{x \in S_+} x \equiv \sum_{x \in S_-} x \pmod{2^n + 1}$$

The elements of S_+ and S_- are powers of two of the form 2^k with $0 \le k \le n-1$. Therefore we have

$$0 \le \sum_{x \in S_+} x \le 2^n - 1$$

and similarly for S_-. This implies that the equality above actually holds as equality of integers:

$$\sum_{x \in S_+} x = \sum_{x \in S_-} x$$

Since the summands are powers of two, and the same power cannot appear twice on one side, it follows that $S_+ = S_-$.[8] In particular, the sets have the same number of elements, which means that the number of summands in (1) is even, which contradicts the fact that p is odd.

We finally managed to derive a contradiction, so our assumption that 2 is a primitive root of unity is false. This completes the "only if" part of the proof.

Exercise 8
We are given $f = x^2 + 2x - 5$ and $g = x^2 + 3x + 2$.

1. We have $N = 17$ and $\omega = 2$. Observe that $17 = 2^{2^2} + 1$, so the previous exercise proves that ω is an 8-th primitive root of unity in $\mathbb{Z}_N$. However, we can also check this directly. The powers of ω in $\mathbb{Z}_{17}$ are

   $$1, 2, 4, 8, 16, 15, 13, 9, 1, \ldots$$

   which shows that ω is an 8-th root of unity.

   Furthermore, $8 \cdot 15 = 120 = 7 \cdot 17 + 1 = 1$, so $8 \in \mathbb{Z}_N^\star$. The last condition for primitive roots states in our case that $\omega^4 - 1$ must not be a zero divisor. In fact, $\omega^4 - 1 = 15 = -\omega \in \mathbb{Z}_N^\star$, so it is not a zero divisor.

[8] Perhaps the most intuitive way to see this is to imagine the numbers written in binary notation. Then the left hand side of the equation is a binary number that has exactly one 1 for every element in S_+.

2. We interpret f as the vector $\begin{pmatrix}12 & 2 & 1 & 0 & 0 & 0 & 0 & 0\end{pmatrix}^T \in \mathbb{Z}_N^8$. Then the discrete Fourier transform can be understood as computing the product

$$\tilde{f} := VDM_\omega \cdot f = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & \omega^7 \\ 1 & \omega^2 & \omega^4 & \omega^6 & 1 & \omega^2 & \omega^4 & \omega^6 \\ 1 & \omega^3 & \omega^6 & \omega & \omega^4 & \omega^7 & \omega^2 & \omega^5 \\ 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 \\ 1 & \omega^5 & \omega^2 & \omega^7 & \omega^4 & \omega & \omega^6 & \omega^3 \\ 1 & \omega^6 & \omega^4 & \omega^2 & 1 & \omega^6 & \omega^4 & \omega^2 \\ 1 & \omega^7 & \omega^6 & \omega^5 & \omega^4 & \omega^3 & \omega^2 & \omega^1 \end{pmatrix} \cdot \begin{pmatrix} 12 \\ 2 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

where all calculations are in $\mathbb{Z}_N$.

It is easy to see that the vector $\tilde{f}$ contains the values of the polynomial of f at the desired support points, i.e.:

$$\tilde{f} = \begin{pmatrix} f(1) \\ f(\omega) \\ f(\omega^2) \\ f(\omega^3) \\ f(\omega^4) \\ f(\omega^5) \\ f(\omega^6) \\ f(\omega^7) \end{pmatrix}$$

Instead of evaluating the matrix product directly, let us use the Fast Fourier Transform. We split f into even and odd parts f_e and f_o, respectively (keeping in mind that the indices are numbered from 0 to 7):

$$f_e = \begin{pmatrix} 12 \\ 1 \\ 0 \\ 0 \end{pmatrix}, f_o = \begin{pmatrix} 2 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

We need to compute their Fourier transforms $VDM_{\omega^2} \cdot f_e$ and $VDM_{\omega^2} \cdot f_o$ recursively.

First, let us compute the Fourier transform of f_e. To do this, we split f_e into even and odd parts f_{ee} and f_{eo}, respectively:

$$f_{ee} = \begin{pmatrix} 12 \\ 0 \end{pmatrix}, f_{eo} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

Now we have to compute their Fourier transforms $VDM_{\omega^4} \cdot f_{ee}$ and $VDM_{\omega^4} \cdot f_{eo}$.

First, let us compute the Fourier transform of f_{ee}. To do this, we split f_{ee} into even and odd parts f_{eee} and f_{eeo}, respectively:

$$f_{eee} = \begin{pmatrix} 12 \end{pmatrix}, f_{eeo} = \begin{pmatrix} 0 \end{pmatrix}$$

The Fourier transforms of those vectors are trivial to obtain, because $\tilde{f}_{eee} = VDM_{\omega^8} f_{eee} = (1) \cdot f_{eee} = f_{eee}$ and similarly $\tilde{f}_{eeo} = f_{eeo}$. We then combine $\tilde{f}_{eee}$ and $\tilde{f}_{eeo}$ to get $\tilde{f}_{ee} = VDM_{\omega^4} \cdot f_{ee}$ per the Fast Fourier transform:

$$\tilde{f}_{ee} = \begin{pmatrix} f_{eee,0} + 1 \cdot f_{eeo,0} \\ f_{eee,0} + \omega^4 \cdot f_{eeo,0} \end{pmatrix} = \begin{pmatrix} 12 \\ 12 \end{pmatrix}$$

Indeed, we can think of f_{ee} as the constant polynomial $12 \in \mathbb{Z}_N[x]$, so $f_{ee}(1) = f_{ee}(\omega) = 12$.

Now let us compute the Fourier transform of f_{eo}. To do this, we split f_{eo} into even and odd parts f_{eoe} and f_{eoo}, respectively:

$$f_{eoe} = (1), f_{eoo} = (0)$$

Similarly to before, their Fourier transforms are easy to get, and the combination step yields

$$\tilde{f}_{eo} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

Now we can combine $\tilde{f}_{ee}$ and $\tilde{f}_{eo}$ to get $\tilde{f}_e = VDM_{\omega^2} \cdot f_e$ (in the following $f_{ee,j}$ indicates the j-th component of f_{ee} and so on):

$$\tilde{f}_e = \begin{pmatrix} f_{ee,0} + 1 \cdot f_{eo,0} \\ f_{ee,1} + \omega^2 \cdot f_{eo,1} \\ f_{ee,0} + \omega^4 \cdot f_{eo,0} \\ f_{ee,1} + \omega^6 \cdot f_{eo,1} \end{pmatrix} = \begin{pmatrix} 12 + 1 \cdot 1 \\ 12 + 4 \cdot 1 \\ 12 + 16 \cdot 1 \\ 12 + 13 \cdot 1 \end{pmatrix} = \begin{pmatrix} 13 \\ 16 \\ 11 \\ 8 \end{pmatrix}$$

Let us verify these results. We can identify $f_e = 12 + x \in \mathbb{Z}_N[x]$. Then $f_e(1) = 13$, $f_e(\omega^2) = 16$, $f_e(\omega^4) = 11$ and $f_e(\omega^6) = 8$ indeed hold.

Now let us compute the Fourier transform of f_o. We could do the same long-winded dance as before, or just observe that f_o corresponds to a constant polynomial, so that $\tilde{f}_o = \begin{pmatrix} 2 & 2 & 2 & 2 \end{pmatrix}^T$. Finally, this allows us to combine $\tilde{f}_e$ and $\tilde{f}_o$:

$$\tilde{f} = \begin{pmatrix} f_{e,0} + 1 \cdot f_{o,0} \\ f_{e,1} + \omega \cdot f_{o,1} \\ f_{e,2} + \omega^2 \cdot f_{o,2} \\ f_{e,3} + \omega^3 \cdot f_{o,3} \\ f_{e,0} + \omega^4 \cdot f_{o,0} \\ f_{e,1} + \omega^5 \cdot f_{o,1} \\ f_{e,2} + \omega^6 \cdot f_{o,2} \\ f_{e,3} + \omega^7 \cdot f_{o,3} \end{pmatrix} = \begin{pmatrix} 13 + 1 \cdot 2 \\ 16 + 2 \cdot 2 \\ 11 + 4 \cdot 2 \\ 8 + 8 \cdot 2 \\ 13 + 16 \cdot 2 \\ 16 + 15 \cdot 2 \\ 11 + 13 \cdot 2 \\ 8 + 9 \cdot 2 \end{pmatrix} = \begin{pmatrix} 15 \\ 3 \\ 2 \\ 7 \\ 11 \\ 12 \\ 3 \\ 9 \end{pmatrix}$$

You can verify that these are indeed the values of f modulo N at the desired points.

This was a lot of verbose text to give us the results, but observe that there are very few actual computations being done. By writing everything in a tabular way, we can save a lot of space, so let us do that for the Fast Fourier transform of g. Splitting g recursively into even and odd parts could be written in tabular form like this:

2	2	2	2
3	1	0	0
1	0	1	1
0	0	0	0
0	3	3	3
0	0	0	0
0	0	0	0
0	0	0	0

The first column contains g, the second column contains g_e and g_o, the third one contains g_{ee}, g_{eo}, g_{oe}, and g_{oo} in that order, and the final column (which could be omitted, because nothing really happens) contains g_{eee}, g_{eeo}, g_{eoe}, and so on. Now we can continue this table to the right for the combining steps.

2	2	3	6
0	2	6	12
1	1	1	13
0	1	15	5
3	3	3	0
0	3	3	0
0	0	3	6
0	0	3	8

The first column is a copy of the last column in the previous table, corresponding to $\tilde{g}_{eee}$, $\tilde{g}_{eeo}$, $\tilde{g}_{eoe}$, and so on, then the second column contains $\tilde{g}_{ee}$, $\tilde{g}_{eo}$, $\tilde{g}_{oe}$, and $\tilde{g}_{oo}$ in that order, and so on. At each step, you can verify that the resulting values are the values of the corresponding polynomial evaluated at the appropriate power of ω.

3. As is known from the lecture, $(VDM_\omega)^{-1} = \frac{1}{n} \cdot VDM_{\omega^{-1}}$. Note that the powers of ω^{-1} are just the powers of ω in reverse order, in particular, $\omega^{-1} = \omega^7 = 9$:

$$1, 9, 13, 15, 16, 8, 4, 2, 1, \ldots$$

First, let us compute the values of $(f \cdot g)(\omega^i) \in \mathbb{Z}_N$.

$$h = f \star g = \begin{pmatrix} 15 \\ 3 \\ 2 \\ 7 \\ 11 \\ 12 \\ 3 \\ 9 \end{pmatrix} \star \begin{pmatrix} 6 \\ 12 \\ 13 \\ 5 \\ 0 \\ 0 \\ 6 \\ 8 \end{pmatrix} = \begin{pmatrix} 15 \cdot 6 \\ 3 \cdot 12 \\ 2 \cdot 13 \\ 7 \cdot 5 \\ 11 \cdot 0 \\ 12 \cdot 0 \\ 3 \cdot 6 \\ 9 \cdot 8 \end{pmatrix} = \begin{pmatrix} 5 \\ 2 \\ 9 \\ 1 \\ 0 \\ 0 \\ 1 \\ 4 \end{pmatrix}$$

Now we apply the Fast Fourier transform to the vector h to compute $VDM_{\omega^{-1}} \cdot h$. Here is the resulting table of intermediate values, analogous to the table-based approach shown at the end of the second part when we computed the transform of g.

5	5	5	5	5	15	5
2	9	0	0	5	7	14
9	0	9	9	10	12	7
1	1	1	1	8	3	6
0	2	2	2	2	7	8
0	1	0	0	2	14	0
1	0	1	1	5	14	0
4	4	4	4	14	7	0

Now we multiply the results with the inverse of $n = 8$, which is $15 = -2 \in \mathbb{Z}_N$, as we have seen in the first part. The resulting vector is

$$\begin{pmatrix} 7 & 6 & 3 & 5 & 1 & 0 & 0 & 0 \end{pmatrix}^T$$

from which we can read off that

$$fg = x^4 + 5x^3 + 3x^2 + 6x + 7 \in \mathbb{Z}_N[x]$$

By actually performing the multiplication manually in $\mathbb{Z}[x]$, we get that

$$fg = x^4 + 5x^3 + 3x^2 - 11x - 10 \in \mathbb{Z}[x]$$

As expected (and we can even use this to double-check that we made no mistake in the calculations), the polynomials are equal when we look at coefficients modulo N. However, if we had only the coefficients modulo N, how could we tell that some of the coefficients of the product in $\mathbb{Z}[x]$ are actually negative?

The answer is that we couldn't. As long as we don't actually do multiplication in $\mathbb{Z}[x]$ by hand–and that would defeat the purpose of using Fast Fourier transforms in the first place–we need some upper bound on the absolute value of the coefficients of $fg \in \mathbb{Z}[x]$. Let's use $|\cdot|$ to denote the maximum absolute value of the coefficients of a polynomial and let us consider the absolute value of the k-th coefficient of fg:

$$|(fg)_k| = \left| \sum_{i=0}^{k} f_i g_{k-i} \right| \leq \sum_{i=0}^{k} |f_i| \cdot |g_{k_i}| \leq (k+1)|f| \cdot |g|$$

In fact, instead of $(k+1)$ we can use the number of non-zero coefficients of f or g, whichever has fewer of them. In our case, that gives us an upper bound

$$|fg| \leq 3 \cdot |f| \cdot |g| = 3 \cdot 5 \cdot 3 = 45$$

So for all we know without doing more analysis, the coefficients of fg could take any integer value between -45 and 45, or $2 \cdot 45 + 1 = 91$ different possible values, whereas $\mathbb{Z}_{17}$ has only 17 elements. Clearly, some information is lost by taking everything modulo 17. Had we chosen $N = 2^{2^4} + 1 = 257$ and $\omega = 4$, all computations would have been the same except for computing modulo 257 instead of modulo 17 (because 4 is an 8-th primitive root of unity modulo 257), and we could have read off fg from the Fourier transform result.