Roots of Unity, Cyclotomic Polynomials and Applications

The task to be done here is to give an introduction to the topics in the title. This paper is neither complete nor very rigorous concerning the proofs. It's a kind of brainstorming. Although roots of unity are easy to define, they are quite involved objects. Nevertheless I believe you should know how to work with them, because they lead to powerful tools in number theory and the theory of polynomials.

A complex number α is called a *n-th root of unity* if $\alpha^n = 1$. Equivalently we can say that the n-th roots of unity are precisely the complex zeros (=roots) of the polynomial $x^n - 1$. This polynomial does not have multiple roots, therefore there are exactly n such numbers. It is easily seen that the product of two n-th roots of unity (rou for short) is again an n-th rou, and a simple check shows that the set of these is in fact a commutative group of order n, which we denote by μ_n. Explicitly by de Moivres formulas the n-th rou are given by $\alpha = e^{2k\pi i/n}$, $0 \leq k \leq n-1$, which means that the all have absolute value 1 and the argument is a multiple of $2\pi/n$. Therefore the are the vertices of a regular n-gon inscribed into the unit circle.

We define the *order* of a rou α to be the smallest positive integer n, such that $\alpha^n = 1$. We call a n-th rou *primitive* if its order is exactly n. There exists a primitive n-th rou, for example $\alpha = e^{2\pi i/n}$. Because $1 \in \mu_n$ is the neutral element of this group, the order of α in our sense is the same as the order of α as an element of the group μ_n. Especially, the existence of a primitive n-th rou implies that the group μ_n is cyclic, meaning that each element of μ_n can be written as a power α^k of a primitive n-th rou α. Another consequence is that the order of $\alpha \in \mu_n$ does not depend on n.

Lemma 0.1. *Let α be a root of unity.*

(a) *Let d be the order of α and let k be an integer. The order of α^k equals $d/(k,d)$.*

(b) *If α is a primitive n-th rou, then α^k is a primitive n-th rou if and only if $(k,n) = 1$. There are exactly $\varphi(n)$ primitive n-th rou (Euler φ-function)*

(c) *We have $\alpha \in \mu_n$ if and only if the order d of α is a positive divisor of n.*

Proof. We prove first that $\alpha^m = 1$ if and only if $d \,|\, m$. Write $m = ld + r$ with $0 \leq r < d$. Then $\alpha^m = (\alpha^d)^l \cdot \alpha^r = \alpha^r$. Now by minimality of d we have $\alpha^m = 1$ if and only if $r = 0$.
(a) We may assume $k > 0$. Let e be the order of α^k. Then $(\alpha^k)^e = 1$ and e is minimal with this property. Therefore e is minimal such that ke is divisible by d. Obviously we must have $e = d/(d,k)$.
(b) Is a direct consequence of (a) and the existence of a primitive n-th rou.
(c) This is just a reformulation of the result at the beginning of the proof because $\alpha \in \mu_n \Leftrightarrow$

$\alpha^n = 1$.

□

I hope that all of this looks familiar to you. We have seen a lemma like this in the structural theory of the groups $(\mathbb{Z}/n\mathbb{Z})^*$ where we also defined orders and obtained similar relations. This is no coincidence. The groups μ_m and $(\mathbb{Z}/n\mathbb{Z})^*$ are both finite and commutative. In case there exists a primitive root mod n, the latter is a cyclic group of order $\varphi(n)$ and is structurally identical to $\mu_{\varphi(n)}$. We can make this correspondence more concrete in the following way. Choose a primitive root g mod n and a primitive $\varphi(n)$-th root of unity α and consider the map

$$h : \mu_{\varphi(n)} \to (\mathbb{Z}/n\mathbb{Z})^*, \qquad \alpha^k \mapsto g^k.$$

By definition of g and α this map is well defined and bijective. In addition we have $h(\beta \cdot \gamma) = h(\beta) \cdot h(\gamma)$ for all $\beta, \gamma \in \mu_{\varphi(n)}$. Therefore h is a so called *homomorphism*, it respects the multiplications of both groups. Now by identifying each $\beta \in \mu_{\varphi(n)}$ with its image in $(\mathbb{Z}/n\mathbb{Z})^*$, the multiplications coincide and there is no difference anymore between these two groups. All we know about the first is also true for the second and vice versa. As an example, the number of primitive $\varphi(n)$-th rou in $\mu_{\varphi(n)}$ is the same as the number of primitive roots mod n, because both are characterized as generators of the respective groups, so they correspond by the map h. As a consequence we get that if there exists a primitive root mod n, then the number of such roots equals $\varphi(\varphi(n))$.

Example 1. *Find all natural numbers n such that the polynomial $x^{2n} + x^n + 1$ is divisible by $x^2 + x + 1$.*

Solution. We first give an ad hoc solution requiring no knowledge on rou. An easy check shows that $x^2 + x + 1$ has no multiple roots. Therefore the problem statement is equivalent to the fact that both complex roots of $x^2 + x + 1$ are also roots of $x^{2n} + x^n + 1$. Let a be one of them. then a is also a root of $(x - 1)(x^2 + x + 1) = x^3 - 1$, therefore $a^3 = 1$ (a is a primitive third rou!). We have to check whether or not $A = a^{2n} + a^n + 1 = 0$ and distinguish three cases. If $n = 3k$ then $A = 1 + 1 + 1 \neq 0$. If $n = 3k + 1$ then $A = a^2 + a + 1 = 0$. Finally if $n = 3k + 2$ then $A = a^4 + a^2 + 1 = a + a^2 + 1 = 0$. As result we get that the division is possible if and only if n is not divisible by 3.

We give now a reinterpretation of the above proof in terms rou. We have $a^2 + a + 1 = (a^3 - 1)/(a - 1)$, therefore the roots of this polynomial are precisely the third roots of unity which are not first rou, in other words the two primitive third rou. Analogously we have $a^{2n} + a^n + 1 = (a^{3n} - 1)/(a^n - 1)$, so the roots of this polynomial are the $3n$-th rou which are not n-th rou. We have to find all n, such that the two primitive third rou are of this form. Obviously, they are always $3n$-th rou, so the question reduces to decide when they are even n-th rou. By lemma 1 (c) this is the case if and only if $3 \mid n$.

□

Next we show how rou may used to compute the coefficients of a polynomial knowing its values on the complex unit circle. Let $p(x)$ be a polynomial with arbitrary (complex) coefficients. It is well known that if the degree of p equals d, then p is completely determined by its values on $d + 1$ different points. But how can we reconstruct the coefficients of p explicitly? We

denote by $p[n]$ the coefficient of the term x^n in p. For example $p(x) = x^2 - 2x + 3$, then $p[0] = 3, p[1] = -2, p[2] = 1$ and $p[n] = 0$ for $n \geq 3$.

Lemma 0.2. *Let p be a polynomial and let α be a primitive n-th root of unity. Then we have*

$$\sum_{\beta \in \mu_n} p(\beta) = \sum_{k=0}^{n-1} p(\alpha^k) = n\left(p[0] + p[n] + p[2n] + \ldots\right).$$

Proof. The first equality is a direct consequence of the fact that μ_n is cyclic and α is a generator of this group. If m is a multiple of n, then we have

$$\sum_{k=0}^{n-1} (\alpha^k)^m = \sum_{k=0}^{n-1} 1 = n.$$

If m is not a multiple of n, then $\alpha^m \neq 1$ and by the formula for a geometric series we get

$$\sum_{k=0}^{n-1} (\alpha^k)^m = \sum_{k=0}^{n-1} (\alpha^m)^k = \frac{(\alpha^m)^n - 1}{\alpha^m - 1} = 0$$

This two calculations prove the lemma for the monomials $p(x) = x^m$, $m \geq 0$. The general case now follows from this and repeated application of the facts $(p + q)[n] = p[n] + q[n]$ for any polynomials p, q and $(a \cdot p)[n] = a(p[n])$ for any polynomial p and any complex number a.

□

So what? This has very important applications for the computation of so called *generating functions*. We will not discuss this in detail, but will come back to this later. Generating functions are one of the most powerful tools in combinatorics and often lead to short but a bit stupid solutions of counting problems. The idea behind this concept is the following: Imagine we want to count something. Now define a polynomial or more generally a power series (Taylor series, a kind of infinite polynomial) such that the numbers we are looking for appear as coefficients of the monomials x^n. Now the argument is two sided. One the one hand the above lemma allows us to express certain combinations of these coefficients in terms of roots of unity (more precisely in terms of the values of this function at certain roots of unity). On the other hand it is often possible to compute these rou-expressions in another way, maybe via factorizations etc. We give an example which uses a special feature of third roots of unity.

Example 2. *Let n be a multiple of 3. Compute the sum*

$$\binom{n}{0} + \binom{n}{3} + \binom{n}{6} + \ldots + \binom{n}{n}.$$

Solution. Consider the Polynomial $p(x) = (x + 1)^n$. The sum S in the problem is precisely $p[0] + p[3] + \ldots + p[n]$. By the above lemma we have

$$S = p[0] + p[3] + \ldots + p[n] = \frac{1}{3}\left(p(1) + p(\alpha) + p(\alpha^2)\right),$$

where α is a primitive third rou. We calculate the right hand side in another way. Of course we have $p(1) = (1 + 1)^n = 2^n$. Next we use a special feature on third roots of unity. We may

assume that $\alpha = e^{2\pi i/3} = -1/2 + i\sqrt{3}/2$. Then $\alpha + 1 = 1/2 + i\sqrt{3}/2 = e^{2\pi i/6}$ is a primitive 6-th rou! So we get $p(1+\alpha) = (e^{2\pi i/6})^n$ and this equals 1 if n is even and -1 if n is odd (remember that n is divisible by 3). An analogous calculation gives $p(1+\alpha^2) = 1$ if n is even and $= -1$ if n is odd. Finally

$$S = \frac{2^n + 2(-1)^n}{3}.$$

□

There is an important geometric applications of roots of unity. They form a regular n-gon inscribed in the unit circle, such that $1 \in \mathbb{C}$ is one of the vertices. Therefore, general regular n-gons may be described with roots of unity. Remember that multiplication with a complex number $e^{i\varphi}$ of absolute value 1 describes a rotation of the complex plane with angle φ (counter-clockwise). Therefore, if $a, b \in \mathbb{C}$ are complex numbers, then the points $a + b\alpha$ with $\alpha \in \mu_n$ are the vertices of a regular n-gon with center a and circumradius $|b|$. More precisely, $a + b$ is one of the n vertices. Obviously any regular n-gon may be described in this way, a being unique and b being unique only up to multiplication with an n-th rou. This is why many problems involving regular n-gons may be solved using rou.

Example 3. *(Putnam 55) Let $A_1A_2 \dots A_n$ be a regular n-gon inscribed in the circle of center O and radius R. On the half-line OA_1 choose P such that A_1 is between O and P. Prove that*

$$\prod_{i=1}^{n} |PA_i| = |PO|^n - R^n.$$

Solution. We identify the plane with $\mathbb{C}$. After a translation and a rotation we may assume that the vertices of the n-gon have coordinates $A_i = R\alpha_i$ where α_i, $i = 1, \dots, n$ are the n-th rou, $\alpha_1 = 1$. The coordinate of P is a real number. Let $x > 1$ be such that the coordinate of P is Rx. We have

$$\begin{aligned}
\prod_{i=1}^{n} |PA_i| &= \prod_{i=1}^{n} |Rx - R\alpha_i| = R^n \prod_{i=1}^{n} |x - \alpha_i| \\
&= R^n \left| \prod_{i=1}^{n} (x - \alpha_i) \right| = R^n |x^n - 1| = R^n (x^n - 1) \\
&= (Rx)^n - R^n = |PO|^n - R^n.
\end{aligned}$$

□

Exercises

1. For which n do we have
$$x^2 + x + 1 \,|\, (x-1)^n - x^n - 1?$$

2. (USA 76) Let P, Q, R, S be polynomials such that for all x
$$P(x^5) + xQ(x^5) + x^2 R(x^5) = (x^4 + x^3 + x^2 + x + 1)S(x).$$
Prove that $P(1) = 0$.

3. (Romania 96) Let $n > 2$ be a natural number. Let $f : \mathbb{R}^2 \to \mathbb{R}$ be a function, such that for every regular n-gon $A_1A_2 \ldots A_n$ in the plane

$$f(A_1) + f(A_2) + \ldots + f(A_n) = 0.$$

Prove that f is the zero function.

4. Finitely many points are given on the unit circle so that the product of the distances from any point on the circle to the given points does not exceed 2. Prove that the points are the vertices of a regular polygon.

5. (Shortlist 02) Let m and n be integers > 1. Let $a_1, a_2, \ldots, a_n$ be integers, none of which is a multiple of m^{n-1}. Show that there are integers $e_1, e_2, \ldots, e_n$, not all zero, with $|e_i| < m$ for $1 \leq i \leq n$, such that

$$m^n \mid e_1a_1 + e_2a_2 + \ldots + e_na_n.$$

Now we shall turn to the definition and properties of the cyclotomic polynomials. These give a complete factorization of the polynomials $x^n - 1$ in $\mathbb{Z}[X]$ as we shall see. This is why they are so important. We define the *n-th cyclotomic polynomial* $\Phi_n(x)$ as follows:

$$\Phi_n(x) = \prod_{\alpha}(x - \alpha),$$

where the product is taken over all primitive n-th rou. By definition and lemma 1 (b) this is a normalized polynomial of degree $\varphi(n)$. Moreover, because the roots of $x^n - 1$ are precisely the n-th rou and each of them has an order dividing n by lemma 1 (c) we get the factorization

$$x^n - 1 = \prod_{d\,|\,n,\ d>0} \Phi_d(x).$$

By the way, comparing the degrees on both sides of this equation we get the following formula:

$$\sum_{d\,|\,n,\ d>0} \varphi(d) = n.$$

Funny, isn't it. The important point now is the following deep result:

Theorem 0.3. *Let n be a positive integer.*

(a) *$\Phi_n(x)$ has integer coefficients, so it lies in $\mathbb{Z}[X]$.*

(a) *$\Phi_n(x)$ is irreducible over $\mathbb{Z}$ and therefore also over $\mathbb{Q}$.*

We shall not prove this, although (a) is not too difficult. But (b) requires knowledge in Galois theory which is well beyond our reach. Taken together, the theorem implies that

$$x^n - 1 = \prod_{d\,|\,n,\ d>0} \Phi_d(x)$$

in fact the full factorization in irreducible factors over $\mathbb{Z}$ respectively $\mathbb{Q}$. This has important consequences as we shall see. But first we need a method to compute $\Phi_n(x)$ explicitly, which is rather simple in fact. Using the above formula we can compute them recursively on the number of prime factors of n. To illustrate the method we will do some easy cases. First of all, of course $\Phi_1(x) = x - 1$. Now let p be a prime number. We have $x^p - 1 = \Phi_1(x)\Phi_p(x) = (x-1)\Phi_p(x)$ and therefore

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x + 1,$$

(already in this simple case the irreducibility is quite hard to prove). Next we have for example $x^{p^2} - 1 = \Phi_{p^2}(x)\Phi_p(x)\Phi_1(x) = \Phi_{p^2}(x)(x^p - 1)$ and

$$\Phi_{p^2}(x) = \frac{(x^p)^p - 1}{(x^p - 1)} = x^{p(p-1)} + x^{p(p-2)} + \ldots + x^p + 1.$$

As a last example, let p, q be different primes. We have $x^{pq} - 1 = \Phi_{pq}(x)\Phi_p(x)\Phi_q(x)\Phi_1(x)$, so

$$\Phi_{pq} = \frac{x^{pq} - 1}{(x-1)(x^{p-1} + \ldots + 1)(x^{q-1} + \ldots + 1)},$$

for example

$$\Phi_6 = \frac{x^6 - 1}{(x-1)(x+1)(x^2 + x + 1)} = x^2 - x + 1.$$

Some more formulas are collected in the following lemma:

Lemma 0.4. (a) $\Phi_{p^r}(x) = \Phi_p(x^{p^{r-1}})$ *for* p *prime and* $r > 0$.

(b) $\Phi_n(x) = \Phi_{p_1 \cdots p_s}(x^{p_1^{r_1-1} \cdots p_s^{r_s-1}})$ *for a prime factorization* $n = p_1^{r_1} \cdots p_s^{r_s}$ *with different primes* p_i *and positive exponents* $r_i > 0$.

(c) $\Phi_{2n}(x) = \Phi_n(-x)$ *for* $n \geq 3$ *odd.*

(d) $\Phi_{pn}(x) = \Phi_n(x^p)/\Phi_n(x)$ *for* p *prime and* $p \nmid n$.

Combining (b) and (d) one can compute explicitly all cyclotomic polynomials. We list the first twelve:

$$\begin{aligned}
\Phi_1(x) &= x - 1 \\
\Phi_2(x) &= x + 1 \\
\Phi_3(x) &= x^2 + x + 1 \\
\Phi_4(x) &= x^2 + 1 \\
\Phi_5(x) &= x^4 + x^3 + x^2 + x + 1 \\
\Phi_6(x) &= x^2 - x + 1 \\
\Phi_7(x) &= x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \\
\Phi_8(x) &= x^4 + 1 \\
\Phi_9(x) &= x^6 + x^3 + 1 \\
\Phi_{10}(x) &= x^4 - x^3 + x^2 - x + 1 \\
\Phi_{11}(x) &= x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \\
\Phi_{12}(x) &= x^4 - x^2 + 1
\end{aligned}$$

Most important are the factorizations of polynomials of the form $x^{p^n} - 1$ for a prime p. We get

$$x^{p^n} = \Phi_1(x) \cdot \prod_{k=1}^{n} \Phi_{p^k}(x) = (x-1) \prod_{k=0}^{n-1} \Phi_p(x^{p^k}),$$

concretely for $p = 2$ and $p = 3$ we obtain

$$x^{2^n} - 1 = (x-1) \prod_{k=0}^{n-1} (x^{2^k} + 1), \qquad x^{3^n} - 1 = (x-1) \prod_{k=0}^{n-1} (x^{2 \cdot 3^k} + x^{3^k} + 1).$$

Using cyclotomic polynomials we may also factor other polynomials which are related to $x^n - 1$. For example we get

$$x^n + 1 = \frac{x^{2n} - 1}{x^n - 1} = \left(\prod_{d \,|\, 2n,\, d>0} \Phi_d(x) \right) / \left(\prod_{d \,|\, n,\, d>0} \Phi_d(x) \right).$$

Now write $n = 2^k \cdot m$ with m odd, the last expression equals

$$\prod_{d \,|\, m,\, d>0} \Phi_{2^{k+1} d}(x).$$

Proceeding further, we write $n = 2^k 3^l m$ with m odd and not divisible by 3:

$$\begin{aligned} x^{2n} - x^n + 1 &= \frac{x^{3n}+1}{x^n+1} = \left(\prod_{d \,|\, 3^{l+1}m,\ d>0} \Phi_{2^{k+1}d}(x) \right) / \left(\prod_{d \,|\, 3^l m,\ d>0} \Phi_{2^{k+1}d}(x) \right) \\ &= \prod_{d \,|\, m,\ d>0} \Phi_{2^{k+1}3^{l+1}d}(x). \end{aligned}$$

We will give an application:

Example 4. *(IMO 90) Find all integers $n > 1$, such that $2^n + 1$ is divisible by n^2.*

Solution. We already proved at the last meeting that the smallest prime divisor of n equals 3. Write $n = 3^k m$ with $3 \not| m$. We want to prove that $k = 1$. We set $y = 2^m$ and get from the above factorization

$$\begin{aligned} 2^n + 1 &= y^{3^k} + 1 = \Phi_2(y) \cdot \prod_{l=1}^{k} \Phi_{2\cdot 3^l}(y) \\ &= (y+1) \cdot \prod_{l=0}^{k-1} (y^{2\cdot 3^l} - y^{3^l} + 1) = (2^m + 1) \cdot \prod_{l=0}^{k-1} (2^{2\cdot 3^l m} - 2^{3^l m} + 1). \end{aligned}$$

Now its easy to check that each of the factors on the right hand side is divisible by 3 but not by 9 (use the fact that m is not divisible by 3). So 3^{k+1} is the largest power of 3 dividing $2^n + 1$. On the other hand this must be divisible by n^2 and therefore by 3^{2k}. This gives $2k \leq k+1$ and $k = 1$. Now proceed as in the first step to prove that in fact $n = 3$.

□

Example 5. *(USA 77) Find all pairs (m, n) of positive integers, such that*

$$1 + x + x^2 + \ldots + x^m \,|\, 1 + x^n + x^{2n} + \ldots + x^{mn}.$$

Solution. We have

$$1 + x + x^2 + \ldots + x^m = \frac{x^{m+1} - 1}{x - 1} = \left(\prod_{d \,|\, m+1,\ d>0} \Phi_d(x) \right) / \Phi_1(x) = \prod_{d \,|\, m+1,\ d>1} \Phi_d(x).$$

And analogously

$$\begin{aligned} 1 + x^n + x^{2n} + \ldots + x^{mn} &= \frac{x^{n(m+1)} - 1}{x^n - 1} = \left(\prod_{d \,|\, n(m+1),\ d>0} \Phi_d(x) \right) / \left(\prod_{d \,|\, n,\ d>0} \Phi_d(x) \right) \\ &= \prod_{d \,|\, n(m+1),\ d \not| n,\ d>0} \Phi_d(x). \end{aligned}$$

Because different cyclotomic polynomials are coprime (by definition, they do not share any common complex roots), the first polynomial divides the second if and only if none of the divisors $d > 1$ of $m + 1$ is also a divisor of n (else there would be a factor of the former polynomial that would not occur in the factorization of the latter). But this in turn is true if and only if $m + 1$ and n are coprime, $(m + 1, n) = 1$.

□

Exercises

1. Prove the formulas in Lemma 4 by similar arguments as in the examples. Use induction.
2. Give the complete factorizations of the polynomials $p_n(x) = x^{2^{n+1}} + x^{2^n} + 1$ and $q_n(x) = x^{2^{n+1}} - x^{2^n} + 1$ over $\mathbb{Z}$. Prove that for every positive integer n, the integer $p_n(2)$ has at least n different prime factors.
3. (Shortlist 02) Let $p_1, \ldots, p_n$ be distinct primes > 3. Prove that

$$2^{p_1 p_2 \cdots p_n} + 1$$

has at least 4^n different positive divisors.

Remark: First prove by elementary means that it has at least 2^n different divisors. This is easy by induction. Then try to refine your argumentation to get 4^n.
A fancy approach via cyclotomic polynomials is also possible. The following is quite a deep result which you may use (but hardly prove) here:

If r and s are positive integers, then $\Phi_r(2)$ and $\Phi_s(2)$ are coprime unless one of r, s is divisible by the other and the quotient is a prime power.

With this approach you will get a far better bound for the number of divisors!

Hints for the Exercises on page 5

1. Use third roots of unity, as in the solution to example 1.
2. If x is a fifth root of unity, then the right hand side vanishes. Obtain 4 different equations in this way and try to manipulate them to get $P(1)$.
3. Identify $\mathbb{R}^2$ with $\mathbb{C}$. Describe a regular n-gon with rou as explained in the text. Now to get an equation for $f(z)$, $z \in \mathbb{C}$ arbitrary, consider an n-gon with center z and consider the n translations of it having the vertices of the first n-gon as centers. Then consider the sum aof all $f(a)$ where a runs through all vertices of all n-gons constructed this way. Some points may be counted more than once!
4. Use complex numbers. The given points $z_1, \ldots, z_n$ have absolute value 1. For an arbitrary point z in $\mathbb{C}$ the product of the distances to all z_i is a polynomial function of z. Now use the hypothesis (and lemma 2 if you want) to obtain precise information about the coefficients of this polynomial. Oh, maybe you should perform a rotation first, so you can prescribe the value of $z_1 \cdot z_n$ (with the obvious restriction that this number has absolute value 1 of course).
5. Use a standard box-principle argument for sequences $(e_1, \ldots, e_n)$ with $e_i \geq 0$ (compare IMO 86 Nr 3, IMO 01 Nr 4 or SMO 03 Nr 8). There is a unique case for which this argument breaks down (as in the latter two problems in the bracket). But it is not easy at all to rule out this case. A simple double counting argument is not enough. Instead consider the polynomial

$$p(x) = \prod_{i=1}^{n} (1 + x^{a_i} + x^{2a_i} + \ldots + x^{(m-1)a_i}).$$

If multiplied out, what are the exponents? What do you know additionally about them? Use this to obtain another expression for p where the exponents are determined modulo m^n. Derive a contradiction. This argument is somehow similar to this generating function thing in example 2.

Hints for the Exercises on page 9

1. Use induction on the number of prime factors of n in all cases except for (c). This can be done directly using the definitions.

2. For the first part: express this polynomials in terms of polynomials of the form $x^k - 1$ as in the examples given in the text. For the second part: Knowing the factorization, it would be enough to prove that the factors are pairwise coprime. This is a bit tedious to be done directly. Instead use the building rule for the factorization, which is in fact true much more generally:

   $$(a^2 + ab + b^2)(a^2 - ab + b^2) = a^4 + a^2b^2 + b^4.$$

   Specialized to our specific situation, the two factors on the left hand side are coprime.

3. (Shortlist 02) Use an appropriate factorization as in the last exercise to prove that increasing n by 1 produces a new prime divisor. This already gives the bound 2^n. To get the 4^n one could try to prove that at least 2 new prime factors are produced when increasing n by 1. But this does not seem to be easy at all. Instead prove and use the following additional observation:

   If $n > m$ then the number mn has at least twice as many divisors than m.