

392 HOMEWORK 6

This homework is a little different from normal – I want you to investigate the factorization of $x^n - 1$ over \mathbb{Q} . By the end of the homework you should have formulated several nice conjectures, but you might not be ready to prove them yet. For each of the problems below try to write down clearly what you think is true (i.e. conjectures) and what you actually know is true (i.e. can prove).

1. Make a table showing how the polynomials $(x^n - 1)$ factorize into irreducibles over \mathbb{Q} for each $n = 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12$. Prove that the factors you find really ARE irreducible.
2. For which n is the polynomial $x^{n-1} + x^{n-2} + \cdots + x + 1$ irreducible over \mathbb{Q} ? Make a conjecture and prove it.
3. For which n is the polynomial $x^n + 1$ irreducible over \mathbb{Q} ? Make a conjecture. Can you prove it? Try for a little while but don't worry if you cannot.
4. There are two divisors of the number 2, namely, 1 and 2. There are three divisors of the number 4, namely, 1, 2 and 4. Compute the number of divisors of n for $n = 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12$. What has this got to do with the number of irreducible factors in your table? Make a conjecture – but don't try to prove it since it is rather hard.
5. Let $\phi(n)$ be the biggest degree of an irreducible factor of $x^n - 1$. For instance, $x^4 - 1 = (x - 1)(x + 1)(x^2 + 1)$ so $\phi(4) = 2$. Using your table, compute $\phi(n)$ for $n = 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12$.
6. There is just one unit in \mathbb{Z}_2 , there are two units in \mathbb{Z}_3 and in \mathbb{Z}_4 . Continue this sequence: how many units are there in \mathbb{Z}_n for $n = 4, 5, 6, 7, 8, 9, 10, 11, 12$. Make a conjecture comparing your answers to 5 and 6. We will prove your conjecture in class in a while, so you can assume it is a fact for the remainder of this homework sheet!
7. Prove that for p prime, the number of units in \mathbb{Z}_{p^n} is equal to $p^{n-1}(p - 1)$. (Hint: it is easier to count the number of non-units in \mathbb{Z}_{p^n} first.) Hence, assuming the conjecture you made in 6, you have shown that $\phi(p^n) = p^{n-1}(p - 1)$.
8. What is $\phi(2^k)$? What is the irreducible factor of $x^{2^k} - 1$ of biggest degree? Now (assuming the conjecture you made in 6 is true) prove for any n that $x^n + 1$ is irreducible if and only if n is a power of 2.