CHM: A.7

Po-Shen Loh

8 April 2001

Problem 1 (A.7) *Let I be an ideal of $\mathbb{Z}[x]$ such that the elements of I do not have a gcd of degree greater than 0 and I contains a polynomial with constant term 1. Prove that I contains the polynomial $1 + x + x^2 + x^3 + \cdots + x^{r-1}$ for some natural number r.*

Solution:

First observe that by the same method of proof as Gauss's Lemma, we can find that any prime factorization of an integral polynomial has the same form (i.e. same number of factors of each degree) as its prime factorization in the fraction field $\mathbb{Q}[x]$.

Lemma 1 *The above statement is true.*

Proof:

To see this, consider a polynomial $f' \in \mathbb{Z}[x]$ that factors into $g'h'$ in $\mathbb{Q}[x]$. Decompose into $\mathbb{Z}[x]$ primitives as follows:

$$\begin{aligned} f' &= Af \\ g' &= \frac{a_1}{a_2} g \\ h' &= \frac{b_1}{b_2} h, \end{aligned}$$

where now all constants and polynomials are integral. Without loss of generality, suppose that the two fractions are already in reduced form. Cross multiply:

$$a_2 b_2 A f = a_1 b_1 g h \tag{1}$$

Now use the fact that $\mathbb{Z}[x]$ is a UFD; pass to the quotient ring $\mathbb{Z}[x]/(a_2)$. The LHS drops out, so a_2 must divide the RHS. Since g, h are primitive and a_1/a_2 is a reduced fraction, it must divide b_1. Similarly, $b_2 | a_1$. Therefore, we can write $f' = AF = Kgh$ for some $K \in \mathbb{Z}$, and any factorization over $\mathbb{Q}$ translates into one over $\mathbb{Z}$ that is of the same form.

Lemma 2 $|I \cap \mathbb{Z}| \neq 0$.

Proof:

By the above, since the gcd of I's elements is in $\mathbb{Z}$, the gcd of I's elements as viewed over $\mathbb{Q}$ is also of degree 0. Since $\mathbb{Q}[x]$ is Euclidean, if $g = (f, h)$ then there exist $a, b \in \mathbb{Q}[x]$ such that $g = af + bh$. We are told that there exists an element in I whose constant term is 1. Start with this one and find another element that it does not divide. We are guaranteed the existence of such an element because the gcd of I's elements is of degree 0. Then from our knowledge in $\mathbb{Q}[x]$ we can write a decomposition like $g = af + bh$. Clearing denominators, we get something of the form $g' = a'f + b'g$ where all polynomials are over $\mathbb{Z}$. Note that the degree of g' is equal to that of g. But since we have an ideal, we know that $g' \in I$.

Continue the process by doing it do g' now. Each iteration reduces the degree by 1, so eventually we will reach degree 0. Therefore, I contains some element $k \in \mathbb{Z}$. Now we know that I contains both a polynomial p with $p(0) = 1$ and an integer k. This amount of knowledge will suffice to solve our problem.

Lemma 3 *I contains a polynomial with constant term 1 whose leading term is relatively prime to k.*

Proof:

Since $k \in I$ we can work in $\mathbb{Z}_k[x]$. Let p be the polynomial with constant term 1. We propose an algorithm that will yield another polynomial with constant term 1 whose leading coefficient has a lesser gcd with k.

Let us represent our polynomials by ordered n-tuples, where $n - 1$ is the degree of the polynomial. For example, represent $x^3 + 2x^2 + 1$ as $(1, 2, 0, 1)$. We will find a polynomial $a \in \mathbb{Z}_k[x]$ such that ap fulfills our algorithmic goal. When we make a, we do not determine the degree first; rather, we build its n-tuple from left to right and determine its degree when it terminates.

Suppose we are not yet done, i.e., we don't have relative primality. Start with the leading coefficient. Our mini-goal within the algorithm will be to make zeros in the leading powers of ap (as viewed over $\mathbb{Z}_k$). Let $p = \sum_0^n p_i x^i$. Let our new polynomial $a = (a_1, a_2, a_3, \ldots, a_m)$. Take note of the fact that our indexing of a is opposite that of p. Let the product $ap = b = (b_1, b_2, \ldots, b_l)$.

We want to get a zero, and we know that $(p_n, k) \neq 1$. Choose $a_1 = k/(p_n, k)$. We get a zero for b_1. Keep going; we want $b_2 = 0$, so choose a_2 such that $a_1 p_{n-1} + a_2 p_n = 0$. Perhaps this is not possible—then we will have b_2 such that it is not a multiple of p_n. Stop now and fill the rest of b with a bunch of zeros (enough so that we don't have to worry about any other terms). An appropriate linear combination of b and p will get a leading term that has smaller gcd. Multiply this by a sufficiently high power of x and add p; this will complete an iteration of our algorithm.

If it was possible to get zero for b_2, then keep going. Eventually we get stuck: this is what we must prove now.

Sublemma 1 *We will get stuck.*

Proof:

Suppose we do not get stuck. Then we will be able to make an arbitrarily long sequence of leading zeros in our product polynomial. After going on for some time, let us switch gears and try something else. That is, now each time we extend our a_i sequence by one term, consider what our product would be if we terminated the a_i sequence right there. It would have degree less than that of p. Now, we are working in the finite ring $\mathbb{Z}_k$, so there are only finitely many such polynomials. We'll eventually see the same polynomial twice.

Suppose that these correspond to the $\mathbb{Z}_k[x]$ polynomials α_1 and α_2, and we have that $\alpha_1 p = \alpha_2 p$. Suppose that α_2 is the one of greater degree (i.e. the one we found last). Take the difference $\alpha = \alpha_2 - \alpha_1$. Now $\alpha p = 0$. Notice that $k \not| \alpha$ because that would mean that we picked $a_1 = 0$, which we did not.

Yet since $\alpha p = 0$ in $\mathbb{Z}_k[x]$, it follows immediately that if we interpret both polynomials in $\mathbb{Z}[x]$, we will have that $k | \alpha p$. Since the constant term of p is 1, p is primitive; hence $k | \alpha$, which we just proved was impossible. This provides us with the desired contradiction here.

Lemma 4 *I contains a monic polynomial with constant term 1. Call this a* ***bimonic*** *polynomial.*

Proof:

Let p be the polynomial found by the previous lemma. From the relative primality, there exists some integer c such that c times p's leading coefficient is 1 mod k. Therefore, multiply p by $(cx + 1)$; this will yield such a monic polynomial in $\mathbb{Z}_k[x]$, and by adding an appropriate multiple of k we can get the desired monic polynomial.

Lemma 5 *I contains a desired polynomial.*

Proof:

Just do long division with our n-tuples, where we don't determine the degree of the dividend until we find a terminating quotient. Work in $\mathbb{Z}_k$. Divide $(1, 1, 1, 1, \ldots)$ by the bimonic p.

Since $\mathbb{Z}_k$ is finite and the degree of p is finite, we either get a "repeating decimal" or a terminating one. That is, eventually we either finish our division happily or end up repeating again. If we terminate, then we will have found that $p | (1, 1, 1, \ldots, 1)$ and are done. Otherwise, if we repeat, then we will have p dividing two polynomials whose n-tuple representations are long strings of 1's (of different lengths) and whose tails are identical. Take the difference of these; then we have $p | x^t q$ where q is of the desired form.

Yet $\mathbb{Z}[x]$ is a UFD. Since $p(0) = 1$, the polynomial p is not divisible by x. Hence $p | q$, and we are done.