Solutions of Assignment 6
Basic Algebra I

October 29, 2004

Solution of the problem 1. Let us first make the following simple remark:

Remark Let $f(x) \in F[x]$, where F can be any field. If $2 \leq \deg f \leq 3$, then $f(x)$ is reducible in $F[x]$ iff $f(x)$ has a root in F.

Back to the problem, suppose that $f(x) = x^3 - 2$ was reducible in $\mathbb{Q}[x]$. So, f would have a root $r = \frac{a}{b}$ (written in the lowest terms) in $\mathbb{Q}$. Thus we would have

$$\left(\frac{a}{b}\right)^3 = 2 \quad \text{or equivalently} \quad a^3 = 2b^3.$$

This implies that $2 \mid a^3$, hence $2 \mid a$. Writing $a = 2a_1$, we have $8a_1^3 = 2b^3$, or $4a_1^3 = b^3$. This in turn implies that $2 \mid b$, which is a contradiction, because a and b have been chosen to be relatively prime.

Remark Another (easy) way to prove the irreducibility of $f(x)$ would be utilizing the Eisenstein's Criterion with prime number 2:

$$2 \mid -2,\ 2 \mid 0,\ 2 \mid 0, \text{and } 2^2 \nmid -2.$$

Therefore, $f(x) = x^3 + 0x^2 + 0x - 2$ is irreducible in $\mathbb{Q}[x]$.

Solution of the problem 2. Any polynomial of degree **3** in $\mathbb{Z}_2[x]$ is of the form $f(x) = x^3 + ax^2 + bx + c$, where $a, b, c \in \mathbb{Z}_2$. So, there are 8 such polynomials:

$$f_1(x) = x^3,\ f_2(x) = x^3+1,\ f_3(x) = x^3+x,\ f_4(x) = x^3+x+1,\ f_5(x) = x^3+x^2,$$

$$f_6(x) = x^3 + x^2 + 1,\ f_7(x) = x^3 + x^2 + x,\ f_8(x) = x^3 + x^2 + x + 1.$$

$f_1(x),\ f_3(x),\ f_5(x)$ and $f_7(x)$ are clearly reducible. Also, a moment consideration will reveal that

$$f_2(x) = (x+1)(x^2+x+1) \quad \text{and} \quad f_8(x) = (x^2+1)(x+1).$$

Now we check that the rest, namely $f_4(x)$ and $f_6(x)$, are actually irreducible. Because our polynomials are of degree 3, it is enough to show that they have no roots in $\mathbb{Z}_2$ (see the first remark in the solution of problem 1). To check that for example $f_4(x)$ has no roots, just note that $f_4(0) = f_4(1) = 1$. And the same thing for $f_6(x)$. Done!

Solution of the problem 3. Starting with prime number 3 and looking for a root, we see that $f(x) = x^2 + 1$ has no zero in $\mathbb{Z}_3$, hence it is irreducible in $\mathbb{Z}_3[x]$. Next consider 5. This case is actually different. In fact in $\mathbb{Z}_5[x]$ we have the factorization $f(x) = (x+2)(x+3)$. Continuing this way, we find that $f(x)$ is irreducible in $\mathbb{Z}_p[x]$ for $p = 3, 7, 11, 19, 23$ and is reducible for $p = 5, 13, 17$.

Looking for a general pattern, first note that each of the primes 5, 13 and 17 is of the form $4k + 1$, and on the contrary, none of the primes 3, 7, 11, 19 and 23 is in that form. Secondly, observe that

$$5 = 2^2 + 1^2, \ 13 = 3^2 + 2^2, \ 17 = 4^2 + 1^2,$$

while the primes 3, 7, 11, 19 and 23 don't enjoy such property, namely they cannot be represented as a sum of two squares. In fact one has the following beautiful theorem of Fermat:

An odd prime number p is a sum of two square, i.e., $p = a^2 + b^2$, if and only if it is of form $4k + 1$.

For further information look at the solutions of the problems 9, 10 and 11.

Solution of the problem 4. Here is one example: $f(x) = 2x^2 + 4$. Note that $f(1) = f(2) = f(4) = f(5) = 0$. This does not contradict the theorem shown in class that a polynomial in $F[x]$ of degree d has at most d roots and the reason is simple: $\mathbb{Z}_6$ is not a field!

Solution of the problem 5. First of all, we show that $f(x) = x^3 + 2x + 1$ is irreducible in $\mathbb{Z}_3[x]$. To see this, just observe that $f(0), f(1), f(2) \neq 0$. So, $\mathbb{Z}_3[x]/(f(x))$ is a field. To count its cardinality, let us first recall that the set consisting of the zero polynomial and all the polynomials of degree less than 3 is the full set of congruence classes modulo $f(x)$, i.e.,

$$\mathbb{Z}_3[x]/(f(x)) = \{[ax^2 + bx + c] : \ a, b, c \in \mathbb{Z}_3\}.$$

Now since we have 3 choices for each coefficient a, b and c, we conclude that there are exactly $3 \times 3 \times 3 = 27$ such congruence classes. Done!

Solution of the problem 6. Both $f(x)$ and $g(x)$ belong to the same congruence class in $\mathbb{R}[x]/(x^2)$ iff $x^2 \mid f(x) - g(x)$ iff $f(x) - g(x) = x^2 h(x)$ for some polynomial $h(x)$ with real coefficients. If this is the case, it is plain that both $f(x) - g(x)$ and its derivative $f'(x) - g'(x) = 2xh(x) + x^2 h'(x)$ vanish at $x = 0$, i.e., $f(0) = g(0), f'(0) = g'(0)$. Conversely, assume that

$$f(0) = g(0), \ f'(0) = g'(0).$$

Since a polynomial vanishes at $x = 0$ iff it is divisible by x, we deduce from the first equation that $f(x) - g(x) = xu(x)$ for some $u(x)$. Now let us take a look at the derivative: $f'(x) - g'(x) = u(x) + xu'(x)$. The second equation now implies that $u(0) = 0$, so by repeating the same argument, we infer that $u(x) = xh(x)$ for some $h(x)$, hence $f(x) - g(x) = xu(x) = x^2 h(x)$ and we are done.

Solution of the problem 7. This can be done with a trial and error search and here is the answer:

$$[x^2+x+1]^{-1} = [x^2].$$

To verify our answer, notice that since $[x^3+x+1] = [0]$, we have

$$[x^2+x+1][x^2] = [x^4+x^3+x^2] = [x(-x-1)+(-x-1)+x^2] = [1]$$

(**N.B.** $2 = 0$ and $-1 = 1$, because we are working in $\mathbb{Z}_2$.) For another way to look at this problem, go to the solution of the next problem.

Solution of the problem 8. Here you are:

$$[x]^1 = [x],\ [x]^2 = [x^2],\ [x]^3 = [x+1],\ [x]^4 = [x^2+x],$$

$$[x]^5 = [x^2+x+1],\ [x]^6 = [x^2+1],\ [x]^7 = [1].$$

So, the smallest $j > 0$ for which $[x]^j = [1]$ is 7, and therefore $[x]$ is a generator for the multiplicative group of nonzero elements of the finite field $\mathbb{Z}_2[x]/(x^3+x+1)$.

Back to the solution of the previous problem, note that

$$[x^2+x+1][x^2] = [x]^5[x]^2 = [x]^7 = [1]\ !$$

Bonus Questions

Solution of the problem 9. Proof by contradiction. Suppose that x^2+1 factors in $\mathbb{Z}_p[x]$. So, it has a root, a say, in $\mathbb{Z}_p$, i.e., $a^2+1 = 0$ in $\mathbb{Z}_p$. This in turn implies that $p \mid a^2+1$ or equivalently $a^2 \equiv -1 \pmod{p}$. Now since p is odd, we can raise both sides of $a^2 \equiv -1 \pmod{p}$ to the power $\dfrac{p-1}{2}$ to get

$$a^{p-1} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}.$$

Comparing with little Fermat, we infer that

$$1 \equiv (-1)^{\frac{p-1}{2}} \pmod{p}.$$

Since $p > 2$, this is impossible unless the last congruence relation becomes equality, i.e., $\frac{p-1}{2} = 2k$, hence $p = 4k+1$, which is a contradiction.

Solution of the problem 10. Let $p = 1+4m$ be a prime. Using Wilson's theorem and also using the relation $j \equiv -(p-j) \pmod{p}$ for $2m+1 \le j \le p-1$, we have

$$\begin{aligned} 0 &\equiv (p-1)!+1 \\ &\equiv 1 \times \cdots \times (2m) \times (2m+1) \cdots \times (4m) + 1 \\ &\equiv 1 \times \cdots \times (2m) \times (-2m) \times \cdots \times (-1) + 1 \\ &\equiv (-1)^{2m} \left(1 \times \cdots \times (2m)\right)^2 + 1 \\ &\equiv \left((2m)!\right)^2 + 1 \pmod{p}. \end{aligned}$$

Thus, $a = (2m)!$ is a root in $\mathbb{Z}_p$ of the polynomial $x^2 + 1 \in \mathbb{Z}_p[x]$.

Solution of the problem 11. Keeping the notation as the previous problem, let us define the following map

$$\phi : \ \mathbb{Z}_p[x]/(x^2+1) \longrightarrow \mathbb{Z}_p \times \mathbb{Z}_p, \quad \phi([f(x)]) = (f(a), \ f(-a)).$$

Obviously, ϕ is a ring homomorphism (check this!).

We now show that ϕ is one-to-one. So, assume that $\phi([f(x)]) = \phi([g(x)])$. Therefore $f(a) = g(a), f(-a) = g(-a)$ in $\mathbb{Z}_p$. This means that the polynomial $h(x) = f(x) - g(x) \in \mathbb{Z}_p[x]$ has two roots in $\mathbb{Z}_p$, namely $\pm a$. On the other hand, since both $f(x)$ and $g(x)$ have degree < 2, then $h(x)$ is a polynomial of degree at most 1 with two roots in the field $\mathbb{Z}_p$. This is impossible unless either $a = -a$ or $h(x)$ is the zero polynomial. The former, however, implies that $2a = 0$ in $\mathbb{Z}_p$, or equivalently $p \mid 2a$ which is absurd, because $p = 1 + 4m > 2m$ and $a = (2m)!$. So, the latter holds, i.e., $f(x) = g(x)$, hence ϕ is injective.

It remains to show that ϕ is surjective. Take an arbitrary element $(r, \ s)$ in $\mathbb{Z}_p \times \mathbb{Z}_p$. We are looking for a congruence class $[\alpha x + \beta] \in \mathbb{Z}_p[x]$ such that $\phi([\alpha x + \beta]) = (r, \ s)$, or equivalently, looking for a solution in α and β of the following system of equations:

$$a\alpha + \beta = r, \quad - a\alpha + \beta = s.$$

By subtracting, we arrive at $2a\alpha = r - s$. This equation has always the solution $\alpha = (2a)^{-1}(r - s)$ (in $\mathbb{Z}_p$) for α, since $2a$ is nonzero in the field $\mathbb{Z}_p$. Substituting in either of the equations yields the solution $\beta = r - 2^{-1}(r - s) = 2^{-1}(r + s)$ for β. Thus, ϕ is also onto and we are done.