# MATH 103B: SOLUTIONS MIDTERM 2

1. (a) Notice that $p_1(1) = 1 + 4 + 2 = 0$ in $\mathbb{Z}_7$ and $p_2(2) = 4 + 3 = 0$ in $\mathbb{Z}_7$, hence both polynomials are reducible over $\mathbb{Z}_7$. Therefore both $\mathbb{Z}_7[x]/\langle p_1(x)\rangle$ and $\mathbb{Z}_7[x]/\langle p_2(x)\rangle$ are not fields.
   (b) Consider the polynomial $p(x) = x^2 + 1$. Observe that $p(0) = 1$, $p(1) = 2$, $p(2) = 5$, $p(3) = 3$, $p(4) = 3$, $p(5) = 5$ and $p(6) = 2$ in $\mathbb{Z}_7$, hence $p(x)$ is an irreducible polynomial over $\mathbb{Z}_7$ of degree 2. Therefore $\mathbb{Z}_7[x]/\langle p(x)\rangle$ is a field of order $7^2 = 49$.
2. (a) Reducing the polynomial $p(x) = x^3 + 2x + 4$ modulo 3 gives $\overline{p}(x) = x^3 - x + 1$ in $\mathbb{Z}_3[x]$. Observe that $\overline{p}(0) = 1$, $\overline{p}(1) = 1$ and $\overline{p}(2) = 1$ in $\mathbb{Z}_3$, hence $\overline{p}(x)$ is irreducible over $\mathbb{Z}_3$. But this implies that $p(x)$ is irreducible over $\mathbb{Q}$.
   (b) We can apply Eisenstein criterion with the prime $p = 2$ to see that the polynomial $(x + 1)^4 + 1 = x^4 + 4x^3 + 5x^2 + 4x + 2$ is irreducible over $\mathbb{Q}$.
   (c) Observe that the polynomial $p(y) = y^4 + 1$ is irreducible over $\mathbb{Q}$ if and only if the polynomial $p(y + 1)$ is irreducible over $\mathbb{Q}$. But we have just seen in part (b) of this problem that $p(y + 1) = (y + 1)^4 + 1$ is irreducible over $\mathbb{Q}$ (replace $y$ by $x$), hence $p(y)$ is irreducible over $\mathbb{Q}$.
3. Notice that the polynomial $p(x) = (x-1)^3 - 2 = x^3 - 3x^2 + 3x - 3$ has the property that $p(a) = 0$. Applying Eisenstein criterion to $p(x)$ with the prime $p = 3$, we see that $p(x)$ is irreducible over $\mathbb{Q}$, hence it must be the minimal polynomial of $a$ over $\mathbb{Q}$. Therefore $\mathbb{Q}(a) \cong \mathbb{Q}[x]/(p(x))$ is a vector space over $\mathbb{Q}$ of dimension $\deg(p(x)) = 3$. We conclude that $[\mathbb{Q}(a) : \mathbb{Q}] = 3$.
4. (a) We assume that $y \neq 0$, hence $N(y) \neq 0$. Let $y = a + b\sqrt{-d}$ with $a, b \in \mathbb{Z}$. We have $N(y) = a^2 + b^2 d$. If $b \neq 0$, then
$$N(y) = a^2 + b^2 d \geq b^2 d \geq d \geq 4.$$
   If $b = 0$, then $N(y) = a^2$. But the only nonzero integer less then 4 which is a square is 1, hence $N(y) = 1$.
   (b) Suppose by contradiction that 2 is reducible in $\mathbb{Z}[\sqrt{-d}]$. In this case $2 = xy$, where both $x$ and $y$ are elements of $\mathbb{Z}[\sqrt{-d}]$ which are not units. In particular $N(x) \geq 2$ and $N(y) \geq 2$. But we have just seen in part (a) of this problem that in this case $N(x) \geq 4$ and $N(y) \geq 4$. This contradicts $4 = N(2) = N(xy) = N(x)N(y)$. Therefore 2 is irreducible.
   (c) *Solution* 1: Observe that $6 = 2 \cdot 3 = (1 - \sqrt{-5})(1 + \sqrt{-5})$ in $\mathbb{Z}[\sqrt{-5}]$. We have already seen in part (b) of this problem that 2 is irreducible. We claim that also 3, $1 - \sqrt{-5}$ and $1 + \sqrt{-5}$ are irreducible.
   Suppose the contrary, say 3 is reducible. Hence we have $3 = xy$ where both $x$ and $y$ are elements of $\mathbb{Z}[\sqrt{-d}]$ which are not units. In particular $N(x) \geq 2$ and $N(y) \geq 2$. Since $9 = N(3) = N(xy) = N(x)N(y)$, we should have $N(x) = N(y) = 3$. But this contradicts part (a) of this problem. Hence 3 is irreducible in $\mathbb{Z}[\sqrt{-5}]$.

Similarly, if $1 \pm \sqrt{-5}$ is reducible, then $1 \pm \sqrt{-5} = xy$ where both $x$ and $y$ are elements of $\mathbb{Z}[\sqrt{-d}]$ which are not units. In particular $N(x) \geq 2$ and $N(y) \geq 2$. Since $6 = N(1 \pm \sqrt{-5}) = N(xy) = N(x)N(y)$, we must have $N(x) = 2$ and $N(y) = 3$, or viceversa $N(x) = 3$ and $N(y) = 2$. In both cases this contradict part (a) of this problem. Hence $1 - \sqrt{-5}$ and $1 + \sqrt{-5}$ are irreducible in $\mathbb{Z}[\sqrt{-5}]$.

To show that the unique factorization property does not hold for $6 \in \mathbb{Z}[\sqrt{-5}]$, it remains to show that 2 is not an associate of $1 - \sqrt{-5}$ or $1 + \sqrt{-5}$. But this follows immediately from the fact that $4 = N(2) \neq N(1 - \sqrt{-5}) = N(1 + \sqrt{-5}) = 6$.

*Solution* 2: Here is a slightly trickier solution which avoids having to prove irreducibility also for 3 and $1 \pm \sqrt{-5}$:

We have $2 \cdot 3 = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. We already know that 2 is irreducible. If $1 \pm \sqrt{-5}$ were not irreducible, we could write each of them as a product of irreducible elements, say $1+\sqrt{-5} = a_1 \ldots a_r$ and $1-\sqrt{-5} = b_1 \ldots b_s$. If the factorization property held in $\mathbb{Z}[\sqrt{-5}]$, 2 would have to be associate to one of these factors, say $a_1$ for simplicity. Hence $2 = a_1 u$ for some unit, and $4 = N(2) = N(a_1)N(u) = N(a_1)$. But as $a_1$ divides $1 + \sqrt{-5}$, this would imply $4 = N(a_1)$ divides $N(1 + \sqrt{-5}) = 6$, a contradiction.

(d) We know that 2 divides $(1 - \sqrt{-5})(1 + \sqrt{-5}) = 6 = 2 \cdot 3$, but 2 cannot divide $1 - \sqrt{-5}$ or $1 + \sqrt{-5}$ since $N(2) = 4$ does not divide $6 = N(1 - \sqrt{-5}) = N(1 + \sqrt{-5})$. Hence 2 is not prime in $\mathbb{Z}[\sqrt{-5}]$.