Math 4400 Homework 6

Due: Wednesday, July 5th, 2017

Feel free to work with your classmates, but everyone must turn in their own assignment. Please make a note of who you worked with on each problem. Let me know if you find a typo, or you're stuck on any of the problems.

1. (5 points) Let R be a ring and let $r \in R$. Show that $(-1_R) \cdot r = -r$. In other words, show that $(-1_R) \cdot r + r = r + (-1_R) \cdot r = 0_R$.

Solution: By definition of additive inverses, $1_R + (-1_R) = 0_R$. Multiplying both sides by r on the right, we get $(1_R + (-1_R)) \cdot r = 0_R \cdot r$. Using the distributive property on the left-hand-side: $1_R \cdot r + (-1_R) \cdot r = 0_R \cdot r$. Now, by definition of the multiplicative identity, $1_R \cdot r = r$. Also, we proved in class that $0_R \cdot r = 0_R$. Thus we have just proven $r + (-1_R) \cdot r = 0_R$. Since addition is commutative, we see that $(-1_R) \cdot r + r = r + (-1_R) \cdot r$.

2. (10 points) Let ω be a quadratic rational. Prove that $\mathbb{Q}[\omega]$ is a field. (Hint: First prove that $\mathbb{Q}[\omega] = \mathbb{Q}[\sqrt{D}]$ for some $D \in \mathbb{Q}$, and then prove $\mathbb{Q}[\sqrt{D}]$ is a field by "rationalizing the denominator" like we did in class)

Solution: By definition, ω is the root of some polynomial $x^2 + px + q$, where $p, q \in \mathbb{Q}$. Thus we can write

$$\omega = \frac{-p \pm \sqrt{p^2 - 4q}}{2}$$

Let $D = p^2 - 4q$ and suppose $\omega = \dfrac{-p + \sqrt{p^2 - 4q}}{2}$. Then we can write $\omega = \dfrac{-p}{2} + \dfrac{1}{2}\sqrt{D}$. Thus, any element $a + b\omega \in \mathbb{Q}[\omega]$ as

$$a + b\omega = a + b\left(-\frac{p}{2} + \frac{1}{2}\sqrt{D}\right) = \left(a - \frac{pb}{2}\right) + \frac{b}{2}\sqrt{D} \in \mathbb{Q}\left[\sqrt{D}\right]$$

This shows that $\mathbb{Q}[\omega] \subseteq \mathbb{Q}[\sqrt{D}]$. On the other hand, $\sqrt{D} = 2\omega + \dfrac{p}{2}$, so any element $a + b\sqrt{D} \in \mathbb{Q}[\sqrt{D}]$ can be written as:

$$a + b\sqrt{D} = a + b\left(2\omega + \frac{p}{2}\right) = \left(a + \frac{bp}{2}\right) + 2b\omega \in \mathbb{Q}[\omega]$$

This shows $\mathbb{Q}[\sqrt{D}] \subseteq \mathbb{Q}[\omega]$, and so $\mathbb{Q}[\omega] = \mathbb{Q}[\sqrt{D}]$. We assumed here that $\omega = \dfrac{-p + \sqrt{p^2 - 4q}}{2}$, but the same argument works if $\omega = \dfrac{-p - \sqrt{p^2 - 4q}}{2}$. So in any case, we just have to show that $\mathbb{Q}[\sqrt{D}]$ is a field.

If $\sqrt{D} \in \mathbb{Q}$, then $\mathbb{Q}[\sqrt{D}] = \mathbb{Q}$, which is a field. So assume $\sqrt{D} \notin \mathbb{Q}$ and let α be a nonzero element of $\mathbb{Q}[\sqrt{D}]$. We can write $\alpha = a + b\sqrt{D}$ for some $a, b \in \mathbb{Q}$. Since we assumed $\sqrt{D} \notin \mathbb{Q}$, we have $a - b\sqrt{D} \neq 0$, so we compute:

$$\frac{1}{a + b\sqrt{D}} = \frac{a - b\sqrt{D}}{a^2 - b^2 D} = \frac{a}{a^2 - b^2 D} + \frac{-b}{a^2 - b^2 D}\sqrt{D} \in \mathbb{Q}[\sqrt{D}]$$

3. (a) (10 points) Prove that there are infinitely many prime numbers congruent to 2 modulo 3. Hint: proceed by contradiction. Suppose that $S = \{p_1, p_2, \cdots, p_s\}$ is the set of all primes congruent to 2 modulo 3, aside from 2. Consider the number $m = 3p_1p_2\cdots p_s + 2$. Show that m is divisible by a prime congruent to 2 modulo 3, but that at the same time m is not divisible by 2 nor by any element of S.

> **Solution:** Since $m = 3p_1p_2\cdots p_s + 2$, we know that $m \equiv 2 \mod 3$. We know there exist some primes $q_1, \ldots, q_r \in \mathbb{Z}$ such that $m = q_1q_2\cdots q_r$. If any of the q_i is congruent to 0 mod 3, then m is congruent to 0 mod 3. If all the q_i are congruent to 1 modulo 3, then m is congruent to 1 modulo 3. Thus there must be some q_i that's congruent to 2 modulo 3. We can relabel the q's so that $q_1 \equiv 2 \mod 3$. Now, each p_i in S is odd, we know that m is odd as well: it's a bunch of odd numbers multiplied together and added to an even number. So this means q_1 cannot be equal to 2. Thus, q_1 is an odd prime congruent to 2 modulo 3. However, q_1 cannot be any of the elements of S, because m isn't divisible by any element of S (here, it's again important that $2 \notin S$). This is a contradiction.

(b) (2 points) What happens if we try to use the same method to prove there are infinitely many primes congruent to 1 modulo 3? What goes wrong?

> **Solution:** Above, we argued that one of the q_i had to be congruent to 2 modulo 3, since the product of a bunch of numbers congruent to 1 modulo 3 will still be congruent to 1 modulo 3. However, the product of a bunch of numbers congruent to 2 modulo 3 *can* be congruent to 1 modulo 3: for instance, $2 \cdot 2 \equiv 1 \mod 3$. That's where the argument breaks down. It's still true that there are infinitely many primes congruent to 1 modulo 3, but we need to use a fundamentally different method to prove this.

4. (a) (5 points) Find the inverse of $5 + 4i$ in $\mathbb{Z}[i]/7\mathbb{Z}[i]$

> **Solution:** We use the formula: $\alpha^{-1} = \overline{\alpha} \cdot N(\alpha)^{-1}$. Here, $N(\alpha) = 25 - 16i^2 = 25 + 16 = 41$, so we need to find the inverse of 41 modulo 7. Well, $41 \equiv -1$ modulo 7, so $N(\alpha)^{-1} = -1$. Thus $\alpha^{-1} \equiv -5 + 4i \equiv 2 + 4i$.
> Just as a sanity check, we compute $(5 + 4i)(2 + 4i) = 10 + 28i + 16i^2 \equiv 1$

(b) (5 points) Find the inverse of $1 + 2\sqrt{6}$ in $\mathbb{Z}[\sqrt{6}]/7\mathbb{Z}[\sqrt{6}]$.

> **Solution:** Here $N(\alpha) = 1 - 4 \cdot 6 = -23 \equiv 5 \mod 7$. Here it's easy enough to check by "brute force" what the inverse of 5 is mod 7; we see that $3 \cdot 5 = 1 \mod 7$, so 3 is the inverse. Thus $\alpha^{-1} = 3 \cdot (1 - 2\sqrt{6}) = 3 - 6\sqrt{6} \equiv 3 + \sqrt{6}$.

(c) (2 points) Is $2 + 6\sqrt{5}$ invertible in $\mathbb{Z}[\sqrt{5}]/11\mathbb{Z}[\sqrt{5}]$? Why or why not?

> **Solution:** As we discussed in class, it all has to do with the norm of $2 + 6\sqrt{5}$: its norm is $2^2 - 6^2 \cdot 5 = -176 \equiv 0 \mod 11$, so the answer is no.

5. (a) (5 points) Let k be a field of characteristic 0. For all $f(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_0$ in $k[X]$, define the derivative of $f(X)$, denoted $f'(X)$, as $(n \cdot a_n)X^{n-1} + (n-1)a_{n-1}X^{n-2} + \cdots + (2a_2)X + a_1$. Prove that, if $f'(X) = 0$, then $f(X) = c$, for some $c \in k$.

Solution: If $f'(X) = 0$, that means $i \cdot a_i = 0$ for all i, such that $1 \leq i \leq n$. Now, since k has characteristic 0, $i \cdot 1 \neq 0$ for all such i. But we have $i \cdot a_i = (i \cdot 1) \cdot a_i = 0$, so $a_i = 0$ whenever $1 \leq i \leq n$, since fields don't have zero divisors. This shows that $f(X) = a_0 \in k$.

(b) (5 points) Show, by example, that this is not necessarily true if $\operatorname{char} k \neq 0$.

Solution: Take $k = \mathbb{Z}/3\mathbb{Z}$. Then if $f(X) = X^9 + 2X^3 + 1$, we have $f'(X) = 3X^8 + 6X = 0$, even though f is certainly not a constant. This is another one of the big reasons why fields of characteristic p are weird.

6. (a) (5 points) What are all the elements of $(\mathbb{Z}[i])^\times$?

Solution: Let $a + bi \in \mathbb{Z}[i]$ be nonzero. Then $\dfrac{1}{a+bi} = \dfrac{a-bi}{a^2+b^2}$. The only way this can be an element of $(\mathbb{Z}[i])^\times$ is if $(a^2 + b^2) \mid a$ and $(a^2 + b^2) \mid b$. Now, for any integers $n, m \in \mathbb{Z}$, if $n \mid m$ and $m \neq 0$ then we must have $|n| \leq |m|$. On the other hand, $\left|a^2 + b^2\right| \geq |a^2| \geq |a|$. Thus, if $|a^2 + b^2| \leq |a|$, either $a = 0$ or we must have $|a^2 + b^2| = |a|$. But this means $|a^2 + b^2| = |a^2|$ and $|a^2| = |a|$; since $a^2, b^2 \geq 0$, the first equation tells us that $b = 0$. Since $|a^2| = |a|^2$, the second equation tells us that $|a| = 1$. In summary, if $(a^2 + b^2) \mid a$, then either $a = 0$, or $|a| = 1$ and $b = 0$. Similarly, if $(a^2 + b^2) \mid b$, then either $b = 0$, or $|b| = 1$ and $a = 0$. Thus, if $a + bi \in (\mathbb{Z}[i])^\times$, then either $|a| = 1$ and $b = 0$, or $a = 0$ and $|b| = 1$. In other words, $(\mathbb{Z}[i])^\times = \{1, i, -1, -i\}$.

(b) (5 points) Prove that the groups $(\mathbb{Z}[i])^\times$ and $\mathbb{Z}/4\mathbb{Z}$ are isomorphic

Solution: Note that $(\mathbb{Z}[i])^\times = \left\{i^0, i^1, i^2, i^3\right\}$. Let $\varphi : (\mathbb{Z}[i])^\times \to \mathbb{Z}/4\mathbb{Z}$ be the function defined by $\varphi(i^n) = [n]$, for $n = 0, 1, 2, 3$. Then φ is a homomorphism: for any two elements $i^n, i^m \in \mathbb{Z}[i]^\times$,

$$\varphi(i^n i^m) = \varphi(i^{n+m}) = [n + m] = [n] + [m] = \varphi(i^n) + \varphi(i^m)$$

Further, φ is a bijection: $\varphi(1) = [0]$, $\varphi(i) = [1]$, $\varphi(-1) = [2]$, and $\varphi(-i) = [3]$. It's clear that each element of $\mathbb{Z}/4\mathbb{Z}$ gets mapped onto, and that no two elements of $\mathbb{Z}[i]^\times$ get mapped to the same thing.

7. (5 points) Use the Lucas-Lehmer test to show that M_{11} is not prime.

Solution: The Lucas-Lehmer sequence, modulo $2^{11} - 1$, is:

$$\begin{aligned}
s_1 &= 4 \\
s_2 &= 14 \\
s_3 &= 194 \\
s_4 &= 788 \\
s_5 &= 701 \\
s_6 &= 119 \\
s_7 &= 1877 \\
s_8 &= 240 \\
s_9 &= 282 \\
s_{10} &= 1736
\end{aligned}$$

Since $s_{10} \not\equiv 0$, we see that $M_{11} = 2^{11} - 1$ is not prime.

Extra credit

8. (10 points (bonus)) Prove that $\mathbb{Z}[\sqrt{2}]/5\mathbb{Z}[\sqrt{2}]$ and $\mathbb{Z}[\sqrt{3}]/5\mathbb{Z}[\sqrt{3}]$ are isomorphic as rings.

9. (10 points (bonus)) Let F be a field of characteristic 0. Show that F contains a subring isomorphic to $\mathbb{Q}$

10. (10 points (bonus)) Use the Lucas-Lehmer test to determine which of the following Mersenne numbers are prime: M_{19}, M_{23}, and M_{31}