Homework 3 for
UTK – M351 – Algebra I
Spring 2004, Jochen Denzler, MWF 10:10–11:00, Ayres 111

Problem 21:
Write out multiplication tables for the rings $\mathbb{Z}_n$ in the cases $n = 2, 3, 4, 5, 6, 7, 8, 9, 10, 11$. Try to come up with an educated guess to answer the questions:
"For which n does the ring $\mathbb{Z}_n$ have a multiplicative inverse for every nonzero element?"
"For which n does the ring $\mathbb{Z}_n$ have zero divisors?"

If you can answer at minimum one of these questions *and give a reason* for your answer, multiplication tables for $n = 8, 9, 10, 11$ are waived for you. (The idea being that you do as many examples as needed to see what's going on.)

Problem 22:
In this problem, we'll see that the division algorithm can be mimicked in the ring $\mathbb{Z}[i]$, which consists of the numbers $a + bi$ where $a, b \in \mathbb{Z}$ and i is the imaginary unit. You may view this ring either as a subring of $\mathbb{C}$, or as an instance of the class of rings constructed in Problem 5.

Given $a = a_1 + a_2 i \in \mathbb{Z}[i]$ and $b = b_1 + b_2 i \in \mathbb{Z}[i]$ with $b \neq 0$, we want to find $q = q_1 + q_2 i \in \mathbb{Z}[i]$ and $r = r_1 + r_2 i \in \mathbb{Z}[i]$ such that $a = qb + r$ and r "smaller" than b. We cannot require "$0 \leq r < b$" because we do not have an order in the ring $\mathbb{Z}[i]$; a statement "$0 \leq r < b$" would be meaningless. Instead we will use the absolute value of complex numbers and require that $|r|$ is smaller than $|b|$, or, equivalently: $r_1^2 + r_2^2 < b_1^2 + b_2^2$.

Given $a = a_1 + a_2 i \in \mathbb{Z}[i]$ and $b = b_1 + b_2 i \in \mathbb{Z}[i] \setminus \{0\}$, let $\vartheta = \vartheta_1 + i\vartheta_2 \in \mathbb{C}$ be the exact quotient $\vartheta = a/b$. Let q_1 be an integer closest possible to ϑ_1 (there may be several equally good choices) and let q_2 be an integer closest possible to ϑ_2. Let r be the remainder making $a = qb + r$ true

(a) To make sure you understand the principle, find q and r according to the prescription of the preceding paragraphs in the case $a = 517 + 213i$, $b = 11 + 25i$. Check that $r_1^2 + r_2^2$ is indeed less than $b_1^2 + b_2^2$.

(b) Write out explicitly what $a = \vartheta b$ means for a_1, a_2, b_1, b_2 and ϑ_1, ϑ_2. — Write out explicitly what $a = qb + r$ means for a_1, a_2, b_1, b_2, q_1, q_2, r_1, r_2. — What does your prescription about the choice of q imply about the size of $q_1 - \vartheta_1$, $q_2 - \vartheta_2$?

(c) Express r_1 and r_2 in terms of b_1, b_2, $q_1 - \vartheta_1$, $q_2 - \vartheta_2$ and conclude that $r_1^2 + r_2^2 < b_1^2 + b_2^2$.

Problem 23:
Divisibility by 11: To find the remainder of a number when divided by 11, for an integer given in decimal notation, the following rule can be used with the digits: Add the digits from right to left, with *alternating sign*. Add/subtract multiples of 11 as needed or desired. The result (between 0 and 10) is the remainder of the given integer upon division by 11.

Example: $a = 357123946803$; We calculate $c = 3 - 0 + 8 - 6 + 4 - 9 + 3 - 2 + 1 - 7 + 5 - 3 = -3$ Add 11 to get 8 (between 0 and 10): The remainder of a when divided by 11 is therefore 8.

Prove this rule by writing up a claculation in the ring $\mathbb{Z}_{11}$

Problem 24:
Given an integer a, let $Q(a)$ be the sum of its digits. E.g., $Q(37491) = 3 + 7 + 4 + 9 + 1 = 24$. What is

$$Q(Q(Q(4444^{4444}))) \ ?$$

To answer the problem, give a rough estimate how large the number could be at most, and use a calculation in $\mathbb{Z}_9$ as a second piece of information.

Problem 25:
(From p. 96) Carry out the Euclidean algorithm to determine the GCD of $a = 7469$ and $b = 2387$. Use the algorithm to write the GCD as a linear combination of a and b.

Problem 26:
(From p. 97) Prove that $(a, bc) = 1$ if and only if $(a, b) = 1$ and $(a, c) = 1$.

Problem 27:
In the ring $\mathbb{Z}[i]$, find a greatest common divisor of $a = 16 + 2i$ and $b = 14 + 31i$, using repeated division with remainder in analogy to Problem 25.

(Note that I said: **a** GCD, with the indefinite article. If g is a GCD, then $-g$, ig and $-ig$ also are correct solutions. The option of selecting 'the positive one' is not available here.)

Problem 28:
Show that 13 (which is a prime in $\mathbb{Z}$ of course) is *not* a prime in the ring $\mathbb{Z}[i]$. You have to find integers a, b, c, d such that $(a + bi)(c + di) = 13$, but neither of the numbers $a + bi$, $c + di$ should be 1, -1, i or $-i$.

Hint: such numbers are easier to guess (and finding one solution is good enough) than to find systematically; see if you can make $c + di = a - bi$.

Problem 29:
Let's try the ring $\mathbb{Z}[\sqrt{-5}]$ for a change: another subring of $\mathbb{C}$; it consists of all the numbers $a+b\sqrt{-5}$ with $a, b \in \mathbb{Z}$. This one will give us a surprise soon.

First show that the only numbers dividing the identity 1 in this ring are $+1$ and -1: you have to find all integers a, b, c, d such that $(a + b\sqrt{-5})(c + d\sqrt{-5}) = 1$.

Now show that 3 is a prime in this ring, namely that 3 has no divisors but ± 3 and ± 1 of 3 in this ring.

Hint: The task to find all integers a, b, c, d such that $(a + b\sqrt{-5})(c + d\sqrt{-5}) = 1$ (or 3) is simplified a lot if you first multiply this equation with its complex conjugate. If you still get stuck, hand it in as pingpong hwk. (This will be a quick pingpong, unlike the first one.)

Just a note for reminder: Be aware that there is a wealth of things to be learned about these 'exotic' rings of arithmetic like $\mathbb{Z}[i]$ and $\mathbb{Z}[\sqrt{-5}]$. However, we are not pursuing these things in this class, except for the purpose of illustrating the corresponding facts in $\mathbb{Z}$: either you glean a deeper understanding of the definitions, properties and theorems about $\mathbb{Z}$ by exploring their analogs in the less familiar rings, or else the less familiar rings serve as counterexamples to show that seemingly "obvious" properties of $\mathbb{Z}$ are not so obvious and need proof.

You are not expected to get a full picture of the properties of these rings from the homework examples.

Also be aware that the abstract concepts (like ring) arose on the basis of concrete examples, like for instance these rings of numbers; this happened *only after* an understanding had been gained that they share many properties. So in working with these examples, you are actually following (to some small extent at least) the way of the founding fathers of the theory.

Problem 30:
Now that you know the technique from Problem 24, find $Q(Q(Q(5555^{5555})))$. — You may now try to work as efficiently as possible: you first find some small a such that $5555 \equiv a \pmod 9$ (you know that already). Then find a small power k such that $5555^k \equiv a^k \equiv 1 \pmod 9$. Somewhere in your calculation you should then have use for a <u>mod k</u> congruence.

Problem 31:
Here I want you to do an experiment again:
In $\mathbb{Z}_n$ calculate $[a]^k$ for each $n \in \{3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13\}$, each a from 2 to $n-1$, and each k beginning from 1 until the sequence starts repeating. I'll do the first samples for you:

In $\mathbb{Z}_3$: $[2]^1 = [2]$, $[2]^2 = [1]$ and then they start over at $[2]$.

In $\mathbb{Z}_4$: $[2]^1 = [2]$, $[2]^2 = [0]$ and then they're all $[0]$.
$[3]^1 = [3]$, $[3]^2 = [1]$ and then it starts over at $[3]$.

In $\mathbb{Z}_5$: $[2]^1 = [2]$, $[2]^2 = [4]$, $[2]^3 = [3]$, $[2]^4 = [1]$ and then it starts over at $[2]$.
$[3]^1 = [3]$, $[3]^2 = [4]$, $[3]^3 = [2]$, $[3]^4 = [1]$ and then it starts over at $[3]$.
$[4]^1 = [4]$, $[4]^2 = [1]$ and then it starts over at $[4]$.

In $\mathbb{Z}_6$: $[2]^1 = [2]$, $[2]^2 = [4]$, and then they start over at $[2]$.
etc.

Problem 32:
In the previous problem, we didn't table the powers of the congruence classes $[0]$ and $[1]$, because $[0]^k = [0]$ and $[1]^k = [1]$ for all positive k. But below you should include them.

For each of the n in the previous problem, I want you to table the following:
(a) Given n, for which congruence classes $[a]$ is it true that $[a]^k = [1]$ for *some* positive k?
(b) For which n do *all* $[a]$ (except $[0]$) have some power $[a]^k$ that is $[1]$ (with $k > 0$)?
(c) For those n that are not listed in part (b), how many $[a]$ have some power $[a]^k$ that is $[1]$ (with $k > 0$)?
(d) Which *periods* occur in $\mathbb{Z}_n$ for powers of those congruence classes $[a]$ that have $[1]$ among their powers? (By period, I mean the smallest $k > 0$ such that $[a]^k = [1]$.)
(e) For each of the lists under (a)–(d), come up with a conjecture that describes the answer not just as a list, but in terms of a notion discussed in class: Use as many among { prime, relatively prime, gcd, divides, Euler's phi function } as possible.

(If you have difficulty coming up with a conjecture, you may want to try a few more examples in Problem 31, to increase your data basis.)

Problem 33:
Give the isomorphism $\theta : \mathbb{Z}_{12} \to \mathbb{Z}_3 \oplus \mathbb{Z}_4$ explicitly (i.e., table all values). — Likewise for $\theta : \mathbb{Z}_{10} \to \mathbb{Z}_2 \oplus \mathbb{Z}_5$.

Also show that there cannot be an isomorphism $\mathbb{Z}_4 \to \mathbb{Z}_2 \oplus \mathbb{Z}_2$. To do this, observe, for instance, the number of solutions to the equation $x + x = 0$ in either ring. Come up with at least one other equation (using multiplication) that has different numbers of solutions in either ring. (Doing so amounts to giving a second proof that there cannot be an isomorphism $\mathbb{Z}_4 \to \mathbb{Z}_2 \oplus \mathbb{Z}_2$).

Problem 34:
Write up an isomorphism between the rings $\mathcal{P}(M)$ and the ring of functions $f : M \to \mathbb{Z}_2$ (with operations in this ring being defined pointwise).

Alert: Problems 35 and 36 are essay questions. If you do not write some decent text to explain what you are doing, you won't get credit for them. If what you write would make the professor of a language department oscillate between a reddish and a greenish complexion if you turned it in there, you won't get credit for the solution here either.

Problem 35:
If you want to factor an odd 100-digit number n (or see if it is prime), you need a computer software that accommodates such long integers. That's no big deal. Then, for the pedestrian way, you need to test divide this number to search for factors. In the worst case, n is the product of two prime numbers with 50 digits each. — It suffices to check if $p|n$ for all *prime* numbers less than or equal to $\sqrt{n}$. EXPLAIN WHY. — Assume that you do test divisions with all *odd* numbers $\leq \sqrt{n}$ (since you prefer to do a few extraneous test divisions over checking all smaller numbers for primality before the test division). Assume the computer does 10^{15} (a million billions) test divisions within one second. HOW LONG DOES IT TAKE TO FACTOR A 100 DIGIT NUMBER IN THE WORST CASE SCENARIO, IF YOU ARE REALLY WEALTHY AND LET 10000 COMPUTERS RUN AT THE SAME TIME, SHARING THE WORK? How does this time compare with, say, the roughly 4000 years of recorded history since the ancient Babylonians?

Suppose you knew all prime numbers smaller than $\sqrt{n}$ already (a very bold hypothesis indeed) and only needed to do test divisions with them rather than all odd numebrs. By what factor would this reduce the work? You may use the famous (and deep) result that there are approximately $x/\ln x$ many prime numbers below x.

Problem 36:
Continuing the previous problem, you want to check if $2^{n-1} \equiv 1 \pmod{n}$. For if this is *not* the case, then you are sure that n is *not* prime, due to little Fermat. (On the other hand, if it turns out that $2^{n-1} \equiv 1 \pmod{n}$, then n may or may not be a prime. How much resources does it take to carry out this test? More precisely:

(a) You try it the naive way and calculate 2^{n-1} first. HOW MANY DIGITS DOES THIS NUMBER HAVE? To store it in a computer, you could hardly do better than using up one atom in your storage medium for each digit of 2^{n-1}. A realistic rough estimate is 6×10^{23} atoms per ounce. How does the weight of the storage medium needed for storing the number 2^{n-1} compare to a a train cargo of 50 wagons with 200 tons capacity each?

(b) You abandon the direct calculation of 2^{n-1} and instead keep squaring the number 2 as often as needed, always reducing modulo the 100-digit number n whenever feasible. You need capacity to multiply integers with 100 digits each. That's less than 2×100 bytes, and, say 5 times as much for intermediate calculations. The storage requirement fits on a floppy disk lavishly. BUT HOW MANY MULTIPLICATIONS DO YOU NEED, ROUGHLY? How long does it take on a real slug of a computer that does 10 multiplications per second?

Problem 37:
Use modular arithmetic to show that the following determinant is not 0:

$$\begin{vmatrix} 1 & 3 & 5 & 0 & 2 & 4 \\ 5 & 2 & 1 & 2 & 4 & 2 \\ 10 & 5 & 3 & 7 & 1 & 0 \\ -5 & 5 & 15 & 11 & -7 & 10 \\ 15 & 0 & -5 & 20 & 5 & 3 \\ 0 & -10 & 5 & 10 & 3 & 5 \end{vmatrix}$$

Problem 38:
How many zeros exactly are at the end of the decimal representation of the number 93!, written out in digits? Only count the contingent zeros at the end, after the last non-zero digits. For instance, for the number 350102100000, you would count five zeros.