Mathematics 243, section 3 – Algebraic Structures
Exam 2, November 2, 2012

I. Think of $\mathbf{R}^2$ (the set of ordered pairs of real numbers) as the ordinary Cartesian coordinate plane. Let R be the relation on $\mathbf{R}^2$ defined by

$$(x_1, y_1)R(x_2, y_2) \Leftrightarrow x_1^2 + y_1^2 = x_2^2 + y_2^2$$

A) (15) Show that R is an equivalence relation on $\mathbf{R}^2$.

Solution: R is reflexive since for any (x, y), $x^2+y^2 = x^2+y^2$, so $(x, y)R(x, y)$ is true. R is symmetric since if $(x_1, y_1)R(x_2, y_2)$ is true, then $x_1^2+y_1^2 = x_2^2+y_2^2$. But then $x_2^2+y_2^2 = x_1^2 + y_1^2$, so $(x_2, y_2)R(x_1, y_1)$ also. Finally, R is transitive since if $(x_1, y_1)R(x_2, y_2)$ and $(x_2, y_2)R(x_3, y_3)$, then $x_1^2 + y_1^2 = x_2^2 + y_2^2$ and $x_2^2 + y_2^2 = x_3^2 + y_3^2$. Therefore, $x_1^2 + y_1^2 = x_3^2 + y_3^2$, so $(x_1, y_1)R(x_3, y_3)$. (Comment: for relations defined in this fashion, the three properties of an equivalence relation follow from the corresponding properties of the equality relation(!))

B) (5) Draw a picture of the equivalence class $[(3, 4)]$ for this relation.

Solution: We have $3^2 + 4^2 = 25$, so the equivalence class $[(3, 4)]$ is the set of all (x, y) satisfying $x^2 + y^2 = 25$. This is the circle of radius 5 centered at $(0, 0)$ in $\mathbf{R}^2$.

II. (20) Prove by mathematical induction: For all $n \geq 1$,

$$\frac{1}{1\cdot 2\cdot 3} + \frac{1}{2\cdot 3\cdot 4} + \cdots + \frac{1}{n(n+1)(n+2)} = \frac{n(n+3)}{4(n+1)(n+2)}.$$

Solution: The base case is $n = 1$ and the formula is true in that case since

$$\frac{1}{1\cdot 2\cdot 3} = \frac{1}{6} = \frac{(1)(4)}{(4)(2)(3)}.$$

For the induction step, assume

$$\frac{1}{1\cdot 2\cdot 3} + \frac{1}{2\cdot 3\cdot 4} + \cdots + \frac{1}{k(k+1)(k+2)} = \frac{k(k+3)}{4(k+1)(k+2)}$$

and consider the corresponding sum for $n = k + 1$:

$$\frac{1}{1\cdot 2\cdot 3} + \frac{1}{2\cdot 3\cdot 4} + \cdots + \frac{1}{k(k+1)(k+2)} + \frac{1}{(k+1)(k+2)(k+3)}.$$

By the induction hypothesis, this equals

$$\frac{k(k+3)}{4(k+1)(k+2)} + \frac{1}{(k+1)(k+2)(k+3)}.$$

We find a common denominator, add, and factor the numerator to simplify:

$$\begin{aligned}
&= \frac{k(k+3)(k+3)}{4(k+1)(k+2)(k+3)} + \frac{4}{4(k+1)(k+2)(k+3)} \\
&= \frac{k(k+3)(k+3)+4}{4(k+1)(k+2)(k+3)} \\
&= \frac{k^3+6k^2+9k+4}{4(k+1)(k+2)(k+3)} \\
&= \frac{(k+1)(k+1)(k+4)}{4(k+1)(k+2)(k+3)} \\
&= \frac{(k+1)(k+4)}{4(k+2)(k+3)} \\
&= \frac{(k+1)((k+1)+3)}{4((k+1)+1)((k+1)+2)},
\end{aligned}$$

which is what we wanted to show.

III.

A) (15) Give the precise statement of the division algorithm in $\mathbf{Z}$, and prove the existence part.

Solution: The statement is that for all integers a and $b > 0$, there exist unique integers q, r such that

$$a = qb + r \qquad \text{and} \qquad 0 \le r < b. \tag{1}$$

We must show that q, r as in (1) exist. So consider the set of integers

$$S = \{a - qb : q \in \mathbf{Z}\}$$

If $0 \in S$, then $a = qb + 0$ for some q and both parts of (1) are satisfied. So this case is done, and for the rest of the proof we will assume $0 \notin S$.

No matter what the sign of a is, we will always have positive elements in S by taking q negative with sufficiently large absolute value. Hence $S \cap \mathbf{Z}^+ \neq \emptyset$. The Well-Ordering Principle implies that $S \cap \mathbf{Z}^+$ has a smallest element. Call this smallest positive element r. Then we have $r = a - qb$ for some $q \in \mathbf{Z}$ and the first statement in (1) is true since $a = qb + r$. The **remainder** of the proof (cue the laugh-track!) is to show that $0 < r < b$. (Note that we have ruled out the case $r = 0$ above.) If $r \geq b$, then we claim that a contradiction results. This is because

$$\begin{aligned} r \geq b &\Rightarrow a - qb = r \geq b \\ &\Rightarrow a - (q+1)b = r - b \geq 0 \end{aligned}$$

The integer $a - (q+1)b$ is also in the set S by definition. Hence either $0 \in S$ which is ruled out above, or else $r - b > 0$ is in S. But $r - b < r$ since $b > 0$. This is a contradiction to the way we found r (it was supposed to be the smallest positive element in S). Hence if $r \neq 0$, then $0 < r < b$.

B) (15) Use the Euclidean algorithm to find the integer $d = \gcd(456, 120)$ and express d in the form $d = m \cdot 456 + n \cdot 120$ for some integers m, n.

Solution: We have

$$\begin{aligned} 456 &= 3 \cdot 120 + 96 \\ 120 &= 1 \cdot 96 + 24 \\ 96 &= 4 \times 24 + 0. \end{aligned}$$

Hence $\gcd(456, 120) = 24$ (the last nonzero remainder). Applying the extended Euclidean Algorithm table (or otherwise), we find

$$\begin{array}{ccc} & 1 & 0 \\ & 0 & 1 \\ 3 & 1 & -3 \\ 1 & -1 & 4 \end{array}$$

Therefore $24 = (-1)(456) + (4)(120)$ is the equation we want.

C) (15) Find all solutions $x \in \mathbf{Z}$ of the congruence $17x \equiv 5 \bmod 32$.

Solution: Since $\gcd(17, 32) = 1$, we can proceed by finding a multiplicative inverse of 17 mod 32:

$$\begin{aligned} 32 &= 1 \cdot 17 + 15 \\ 17 &= 1 \cdot 15 + 2 \\ 15 &= 7 \cdot 2 + 1 \end{aligned}$$

So

$$\begin{array}{ccc} & 1 & 0 \\ & 0 & 1 \\ 1 & 1 & -1 \\ 1 & -1 & 2 \\ 7 & 8 & -15 \end{array}$$

Therefore $(8)(32) + (-15)(17) = 1$, which says the multiplicative inverse of 17 is $-15 \equiv 17 \bmod 32$. (Note: We can compute $17^2 = 289 = 9 \cdot 32 + 1$, so this is correct.) Then the congruence can be rewritten as

$$x \equiv 17 \cdot 5 \equiv 21 \bmod 32$$

and the solutions in $\mathbf{Z}$ are all the integers of the form $x = 21 + 32\ell$ for $\ell \in \mathbf{Z}$.

IV. (15) Let a, b, c be integers. Show that if $\gcd(a, b) = 1$ and $a|(bc)$, then $a|c$.

Solution 1: If $\gcd(a, b) = 1$, then there exist $m, n \in \mathbf{Z}$ such that $ma + nb = 1$. Multiply both sides of this equation by c to get $(mc)a + n(bc) = c$. Since we assume $a|(bc)$, we know $bc = qa$ for some integer q, and therefore by substitution and rearrangement using commutativity, associativity, and distributivity of multiplication in $\mathbf{Z}$, $c = (mc)a + (nq)a = (mc + nq)a$ This shows $a|c$.

Solution 2: It is also possible to prove this by reasoning along the lines of Euclid's Lemma. However, since *we are not assuming that a itself is prime*, this must be done carefully and no one who tried to do it this way quite saw how to push it through correctly. What is true is that if p is any prime number dividing a, then $p|(bc)$, and Euclid's Lemma shows $p|b$ or $p|c$. However we also assumed that $\gcd(a, b) = 1$, so if $p|a$, then $p \not| b$ and as a result $p|c$. This says $a = pa'$ and $c = pc'$ for some integers a', c'. From the equation $bc = qa$ for some q, we get $bc'p = qa'p$, so $bc' = qa'$ by cancellation. It is true that $\gcd(a', b) = 1$ and $a'|(bc')$. Hence we can repeat the argument with a' and c'. After a finite number of such steps we will have cancelled all the prime factors of a and shown that $a|c$.

Extra Credit (10) Give a proof that every positive integer $n > 1$ is a product of prime numbers using complete induction. (Note: a "product" here may consist of a single factor.)

Solution: The base case is $n = 2$. Since 2 is a prime the statement is true (allowing products with one factor). Now assume the statement is true for all $\ell < n$ and consider n. If n itself is prime, then we are done as in the base case. Otherwise, $n = \ell_1\ell_2$ with $1 < \ell_1, \ell_2 < n$. By the induction hypothesis we can write both ℓ_1 and ℓ_2 as products of primes, and then the same is true for n.