Math 343K (Rusin) Exam 1, Mar 2, 2012: SOME POSSIBLE ANSWERS

1. The *perfect squares* are the numbers in the familiar sequence $1, 4, 9, 16, \ldots$. Show that the sum of the first n perfect squares is $\frac{n(n+1)(2n+1)}{6}$.

Answer: Let $S(n) = 1 + 4 + \ldots + n^2$ and $T(n) = n(n+1)(2n+1)/6$, and let $P(n)$ be the statment "$S(n) = T(n)$". (Note that $S(n)$ and $T(n)$ are NUMBERS, while $P(n)$ is a SENTENCE.)

$P(1)$ is true because $S(1) = T(1) = 1$.

If $P(k-1)$ is a true statement for some integer k, then $P(k)$ is also true: $S(k) = 1+4+\ldots+(k-1)^2+k^2$ is obviously the same as $S(k-1)+k^2$, while $T(k)$ exceeds $T(k-1)$ by $k(k+1)(2k+1)/6-(k-1)k(2(k-1)-1)/6 = (k/6)((2k^2+3k+1)-(2k^2-3k+1)) = k^2$ as well. That is, we have $S(k) = S(k-1) + k^2 = T(k-1) + k^2 = T(k)$, as desired.

Thus $P(n)$ is a true statement for all natural numbers n, by the Principle of Mathematical Induction.

2. Prove that if a, b, c are integers and $\gcd(a, b) = \gcd(a, c) = 1$ then $\gcd(a, bc) = 1$.

Answer: Suppose d is a common divisor of a and bc. If $d > 1$ then d is divisible by some prime p. But then $p|bc$ and so by Euclid's lemma, p must divide either b or c. On the other hand, $p|d$ and $d|a$ means $p|a$ too, so p is a common divisor either of a and b, or of a and c. But both those pairs have no common divisor larger than 1, a contradiction. So $d = 1$, and thus $\gcd(a, bc) = 1$.

Remark: it is cumbersome to say anything useful about $\gcd(a, bc)$ when both $\gcd(a, b)$ and $\gcd(a, c)$ are greater than 1.

3. In this problem, assume that a, b, m, n, x, y are all integers, with $mx + ny = 1$.

3a. Show that $\gcd(m, n) = 1$ and that $ny \equiv 1 \pmod{m}$.

Answer: Any common divisor of m and n would divide both mx and ny and hence their sum, $mx + ny$, which is 1. So the common divisors can only be ± 1.

ny differs from 1 by mx, which is a multiple of m

3b. Show that $u = any + bmx$ satisfies both congruences $u \equiv a \pmod{m}$ and $u \equiv b \pmod{n}$.

Answer: Working first modulo m, we have already seen $ny \equiv 1$, so $any \equiv a$. On the other hand, $m \equiv 0$, so $bmx \equiv 0$ too. Adding shows $u = (any + bmx) \equiv (a + 0) = a$. The proof that $u \equiv b \pmod{n}$ is nearly identical.

Note: By Bezout's theorem, given any coprime pair m, n we can always find such an x and y. Thus whenever $\gcd(m, n) = 1$, we can always find integers u with $u \equiv a \pmod{m}$ and $u \equiv b \pmod{n}$, no matter what a and b. This result is called the *Chinese Remainder Theorem.*

3c. Find four distinct congruence classes $u \in \mathbf{Z}_{77}$ with $u^2 \equiv 1 \pmod{77}$. (*Hint* You need u to be congruent to $+1$ or to -1 modulo 11, and likewise modulo 7.)

Answer: Using the hint, we look for integers u which are on the one hand congruent to either $+1$ or -1 modulo 11, and which are on the other hand congruent to either $+1$ or -1 modulo 7. Obviously $+1$ and -1 are candidates. To get another, we might want an integer u which is, say, congruent to $+1$ modulo 11 but congruent to -1 modulo 7. Well $\gcd(7, 11) = 1$ so we may use the ideas of 3b: a Bezout equation we can use is $7\cdot(3)+11\cdot(-2) = 1$, from which we obtain the solution $u = (1)(7)(3)+(-1)(11)(-2) = 43$. Similarly $u = -43 \equiv 34$ works.

Remark: it's not hard to show that these are the *only* four congruence classes of solutions, because 7 and 11 are prime.

3d. Hey, wait a minute — since $u^2 - 1 = (u - 1)(u + 1)$, shouldn't $u = 1$ and $u = -1$ be the only solutions to the congruence in part (c)? Explain.

Answer: The relationship between factors and roots (of a polynomial) still partially holds in $\mathbf{Z}_n$: if $P(X) = (X - a)(X - b)\ldots$ then $a, b, \ldots$ are all roots of P. But they need not be the only ones: u is a root iff $P(u) \equiv 0$, i.e. iff $(u - a)(u - b)\ldots \equiv 0$. But unlike the real or complex numbers, the integers-modulo-n have *zero-divisors*: it is possible for a product like $(u - a)(u - b)\ldots$ to be zero even when none of the factors is, for example $14 \cdot 33 \equiv 0 \pmod{77}$ even though neither 14 nor 33 is zero.

4a. Show that if G is any group and x and y are any two elements of G, then the group element $z = y^{-1}xy$ has the same order as x.

Answer:

Note first that $z^2 = z \cdot z = (y^{-1}xy)(y^{-1}xy) = y^{-1}x(yy^{-1})xy = y^{-1}xexy = y^{-1}xxy = y^{-1}x^2y$ and similarly (by induction on n, if you like) we see that for $n = 0, 1, 2, \ldots$ we have $z^n = y^{-1}x^ny$.

Now observe that if $n = o(x)$ then $x^n = e$ and so $z^n = y^{-1}ey = e$.

Thus the order of x becomes an upper bound on the order of its *conjugate*, z.

On the other hand, $x = yzy^{-1} = u^{-1}zu$, where $u = y^{-1}$, which is to say that x is also a conjugate of z, and thus by the previous paragraphs we see the order of z is also an upper bound on the order of x. So indeed the two have the *same* order.

4b. Compute z when $G = Sym(6)$, $x = (123)(45)$ and $y = (135)(246)$.

Answer: Remember, xy is the composite function obtained by first performing y and then performing x. In our case this means $1 \to 3 \to 1$, $2 \to 4 \to 5$, $3 \to 5 \to 4$, $4 \to 6 \to 6$, $5 \to 1 \to 2$, and $6 \to 2 \to 3$, i.e. $xy = (1)(25)(346)$. On the other hand $y^{-1} = (642)(531)$, and when we apply this after xy we get the function $y^{-1} \circ xy = (156)(23)(4)$.

Just as a check you might observe that this has the same order as x itself, as required by part (a). In fact it is true in the symmetric groups that x and z will not only have the same order but the same cycle structure. as this example illustrates.

5. In any group G we define the *center* of G to be

$$Z(G) = \{g \in G | \; gh = hg \;\text{ for all} h \in G\}$$

Show that $Z(G)$ is a subgroup of G. (Don't forget to verify that $Z(G)$ is nonempty!)

Answer: $Z(G)$ is not empty because it contains $e : eh = he\ (= h)$.

To see $Z(G)$ is closed under the binary operation, suppose g_1 and g_2 are two elements in $Z(G)$; is $g_3 = g_1 g_2$ in there, too? Well, we would have to check whether $hg_3 = g_3 h$ for all $h \in G$. But indeed $hg_3 = h(g_1 g_2) = (hg_1)g_2 = (g_1 h)g_2 = g_1(hg_2) = g_1(g_2 h) = (g_1 g_2)h = g_3 h$, as desired. (Make sure you understand why each of those "=" statements is true!)

Similarly we must check that $Z(G)$ is closed under inversion. But if $hg = gh$, multiply both sides of this equation (on the left) by g^{-1} to get $g^{-1}hg = g^{-1}gh = h$. Then multiply both sides on the right by g^{-1} to get $g^{-1}h = g^{-1}hgg^{-1} = hg^{-1}$. So g^{-1} also passes the membership to get in to $Z(G)$.