Mathematics 243, section 2 – Mathematical Structures
Solutions for Exam 3 Review Problems
November 29, 2017

Sample Exam Questions

Note: This list is longer than the actual exam will be to show the range of different kinds of questions that might appear. But the exam questions will be similar in content and format.

I. Consider an RSA public key cryptosystem with public information $m = 143$ and $e = 37$.

A) "Crack the system" by determining the private information p, q and d.
Solution: The first step is that we need to factor m, here $m = 143 = 11 \cdot 13$. The two primes are $p = 11$ and $q = 13$. (As we said before, the secure RSA systems used in the real world at the moment have primes p, q of around 200 decimal digits so this first step would be impractical, even with the current fastest computers and best software.) Then recall the encryption and decryption exponents are related by

$$e \cdot d \equiv 1 \bmod (p-1)(q-1).$$

So we need to determine a multiplicative inverse for $e = 37$ in $\mathbf{Z}/120\mathbf{Z}$ (since $(11-1)(13-1) = 10 \cdot 12 = 120$). To do this we use the usual Euclidean algorithm approach:

$$\begin{aligned} 120 &= 3 \cdot 37 + 9 \\ 37 &= 4 \cdot 9 + 1 \end{aligned}$$

Hence with the Extended Euclidean Algorithm table:

$$\begin{array}{ccc} & 1 & 0 \\ & 0 & 1 \\ 3 & 1 & -3 \\ 4 & -4 & 13 \end{array}$$

and the multiplicative inverse of $e = 37$ is $d = 13$.

B) You intercept a message encrypted using this system consisting of the numbers $40, 114$. Use your answer to part A and the table on page 102 of the course notes to decrypt the message.
Solution: We take

$$40^{13} \bmod 143 = 79$$

and

$$114^{13} \bmod 143 = 75$$

From the table, 79 $\leftrightarrow$ "O'' and 75 $\leftrightarrow$ "K''. The decrypted message is "OK" (not so valuable without knowing what the question was :). As a practical matter, to do calculations like this by hand, you would want to use *repeated squaring*. For instance

$$\begin{aligned} 40^2 &\equiv 27 \bmod 143 \\ 40^4 &\equiv 27^2 \equiv 14 \bmod 143 \\ 40^8 &\equiv 14^2 \equiv 53 \bmod 143 \end{aligned}$$

Hence

$$40^{13} \equiv 40^8 \cdot 40^4 \cdot 40 \equiv 53 \cdot 14 \cdot 40 \equiv 79 \bmod 143.$$

II.

A) Give the statement and proof of "Fermat's Little Theorem."
Solution: The statement is: If p is prime and $\gcd(a,p) = 1$, then $a^{p-1} \equiv 1 \bmod p$. Here's a sketch of the proof we did in class (try to fill in details for unproved statements yourself!). Since $\gcd(a,p) = 1$, we know $[a]$ has a multiplicative inverse mod p. This implies that the mapping $f : (\mathbf{Z}/p\mathbf{Z})^\times \to (\mathbf{Z}/p\mathbf{Z})^\times$ is both injective and surjective. Hence,

$$1 \cdot 2 \cdot \cdots \cdot (p-1) \equiv a \cdot (2a) \cdot (3a) \cdot \cdots \cdot (a(p-1)) \bmod p$$

But the right side is just $a^{p-1} \cdot (1 \cdot 2 \cdot \cdots \cdot (p-1))$, so we have

$$x \equiv x \cdot a^{p-1} \bmod p \tag{1}$$

where $x = (p-1)! = 1 \cdot 2 \cdot \cdots \cdot (p-1)$. Now $\gcd(x,p) = 1$ as well since all the factors are strictly less than p and p is prime. Hence x also has a multiplicative inverse mod p, and we can multiply both sides of (1) by that multiplicative inverse to get

$$1 \equiv a^{p-1} \bmod p,$$

which is what we wanted to show.

B) Use part A to compute $3^{177} \bmod 7$.
Solution: We have $3^2 \equiv 2 \bmod 7$, $3^3 \equiv 6 \bmod 7$, $3^4 \equiv 4 \bmod 7$, $3^5 \equiv 5 \bmod 7$ and $3^6 \equiv 1 \bmod 7$ (also by Fermat's Little Theorem from part A). Therefore $3^{177} \equiv 3^{177 \bmod 6} \equiv 3^3 \equiv 6 \bmod 7$.

C) What is the *smallest* positive power k such that $7^k \equiv 1 \bmod 11$? Same question for $5^k \equiv 1 \bmod 11$.
Solution: $7^{10} \equiv 1 \bmod 11$ but no smaller positive power is congruent to 1 mod 11. $5^5 \equiv 1 \bmod 11$. This says $k = 5$ is the smallest such positive power.

III. Let $f : A \to B$ be a mapping.

A) If $S, T \subseteq A$ and $f(S) \cap f(T) \neq \emptyset$, can you conclude that $S \cap T \neq \emptyset$? (The answer is: No). Why not? Give a counterexample.
Solution: The answer is: No. The reason is that there is nothing here that would say f has to be *injective*. Let $A = \{a, b\}$ (where $a \neq b$) and let $B = \{y\}$, define

$f : A \to B$ by making $f(a) = y = f(b)$. If $S = \{a\}$ and $T = \{b\}$, then $S \cap T = \emptyset$, but $f(S) = f(T) = \{y\}$ so $f(S) \cap f(T) \neq \emptyset$.

B) (continuing from A) Give a condition on f that would imply $S \cap T \neq \emptyset$ under the assumption that $f(S) \cap f(T) \neq \emptyset$. Prove your assertion.
Solution: From the counterexample in part A, we expect that if f is assumed to be injective, then $f(S) \cap f(T) \neq \emptyset$, then $S \cap T \neq \emptyset$. To prove this suppose $y \in f(S) \cap f(T)$, then $y = f(a)$ for some $a \in S$ and also $y = f(b)$ for some $b \in T$. But then $f(a) = f(b)$. If f is injective, this implies $a = b$, so both are in S and in T, hence in $S \cap T$.

C) If $U, V \subseteq B$ and $f^{-1}(U) \cap f^{-1}(V) \neq \emptyset$, can you conclude that $U \cap V \neq \emptyset$? If so, prove it. If not, give a counterexample.
Solution: Yes you can. If $f^{-1}(U) \cap f^{-1}(V) \neq \emptyset$, then there is some $x \in f^{-1}(U)$ for which $x \in f^{-1}(V)$ is also true. This means $f(x) \in U$ and $f(x) \in V$, so $U \cap V \neq \emptyset$, since $f(x) \in U \cap V$.

D) Show that f is surjective if and only if there is a mapping $g : B \to A$ such that $f \circ g = id_B$. ($id_B : B \to B$ is the mapping satisfying $id_B(y) = y$ for all $y \in B$.)
Solution: $\Rightarrow$: if f is surjective, then for each $y \in B$, there is some $x \in A$ such that $f(x) = y$. Define $g : B \to A$ by saying $g(y) = x$ where $f(x) = y$. If there is more than one possible x, just take any one of them and use that to define g. But now if $y \in B$ is arbitrary $(f \circ g)(y) = f(g(y)) = f(x) = y$. Hence $f \circ g = id_B$.

$\Leftarrow$: If there is a g such that $f \circ g = id_B$, then for all $y \in B$, $y = id_B(y) = (f \circ g)(y) = f(g(y))$. But this says that $f(x) = y$ where $x = g(y) \in A$. Hence g is surjective because $y \in B$ was arbitrary.

IV.

A) The binomial coefficient $\binom{n}{k}$ is the number of subsets of $A = \{a_1, \ldots, a_n\}$ that contain exactly k elements. Assuming this fact, give (yet another) proof that A has 2^n distinct subsets (including $\emptyset$ and A itself).
Solution: The Binomial Theorem says

$$(x + y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

Substitute $x = y = 1$ to get

$$2^n = \sum_{k=0}^{n} \binom{n}{k} 1^k \cdot 1^{n-k} = \sum_{k=0}^{n} \binom{n}{k}.$$

There are $\binom{n}{k}$ different ways to select a subset of A containing exactly k elements for each $k = 0, \ldots, n$. This accounts for all of the subsets since every subset has one of these integers k as its number of elements. Hence the number of subsets is the sum, which equals 2^n.

B) Show by mathematical induction: For all $u > 0$ in the reals, and all $n \geq 0$,

$$1 + nu + \frac{n(n-1)}{2}u^2 + \frac{n(n-1)(n-2)}{6}u^3 \leq (1 + u)^n$$

Solution: The idea is the same as Exercise 9.18 from Problem Set 8. For the induction step, use the induction hypothesis like this:

$$(1+u)^{k+1} = (1+u)^k \cdot (1+u) \geq \left(1 + ku + \frac{k(k-1)}{2}u^2 + \frac{k(k-1)(k-2)}{6}u^3\right)(1+u)$$

Multiply out and simplify. You will see that the result is

$$1 + (k+1)u + \frac{(k+1)k}{2}u^2 + \frac{(k+1)k(k-1)}{6}u^3 + (\textit{positive})$$

This implies the statement with $n = k+1$.

C) Give a second proof of the statement in part B using the Binomial Theorem.
Solution: See part B Exercise 9.18 from Problem Set 8. This follows because the

$$1 + nu + \frac{n(n-1)}{2}u^2 + \frac{n(n-1)(n-2)}{6}u^3$$

exactly equals the first four terms in the binomial expansion of $(1+u)^n$ and the remaining terms are all non-negative.

V.

A) Prove that $\mathbf{N}$ is not bounded above in the real numbers. Use this to deduce that for any $\varepsilon > 0$, there exists $n \neq 0 \in \mathbf{N}$ such that $\frac{1}{n} < \varepsilon$.
Solution: Suppose on the contrary that $\mathbf{N}$ is bounded above in $\mathbf{R}$. Then the Completeness Axiom implies that $\mathbf{N}$ has a least upper bound, say B. Since $B - 1 < B$, this would imply that there must be a natural number $n \in \mathbf{N}$ satisfying $B - 1 < n \leq B$. However given n, $n + 1 \in \mathbf{N}$ as well, and by adding 1 to the two terms on the left in the last inequalities, $B < n + 1$. This contradicts the choice of B since B was supposed to be an upper bound for $\mathbf{N}$. For the second part, if $\varepsilon > 0$, then $1/\varepsilon$ is not an upper bound for $\mathbf{N}$, so there exists $n \in \mathbf{N}$ with $n > 1/\varepsilon$. Since $n, 1/\varepsilon > 0$, this implies $1/n < \varepsilon$, which is what we wanted to show.

B) Use the last statement in part A to prove that the sequence $a_n = 3 - \frac{1}{n}$ converges to $L = 3$.
Solution: Let $\varepsilon > 0$ and use the previous part to find $n_0 \in \mathbf{N}$ such that $1/n_0 < \varepsilon$. Then for any $n \geq n_0$ we have

$$\left|(3 - \frac{1}{n}) - 3\right| = \frac{1}{n} \leq \frac{1}{n_0} < \varepsilon.$$

This shows that a_n converges to 3 by the definition.

C) Prove that $a_n = 3 - \frac{1}{\sqrt{n}}$ also converges to $L = 3$.
Solution: Let $\varepsilon > 0$ and use the previous part to find $n_0 \in \mathbf{N}$ such that $1/n_0 < \varepsilon^2$. This implies $n_0 > 1/\varepsilon^2$, so $\sqrt{n_0} > 1/\varepsilon$ and $1/\sqrt{n_0} < \varepsilon$. Then for any $n \geq n_0$ we have

$$\left|(3 - \frac{1}{\sqrt{n}}) - 3\right| = \frac{1}{\sqrt{n}} \leq \frac{1}{\sqrt{n_0}} < \varepsilon.$$

This shows that a_n converges to 3 by the definition.

VI. Let R be the relation on the set of real numbers defined by aRb if and only if $a - b \in \mathbf{Z}$. For example $1.32R(-5.68)$ is true for this relation since $1.32 - (-5.68) = 7 \in \mathbf{Z}$.

A) Show that R is an equivalence relation.
Solution:
- R is reflexive since for every real number x, $x - x = 0 \in \mathbf{R}$.
- R is symmetric since if xRy, then $x - y \in \mathbf{Z}$, so $-(x - y) = y - x \in \mathbf{Z}$ as well. (The set of integers is closed under taking additive inverses.) This shows yRx.
- R is transitive since if xRy and yRz, then $x - y$ and $y - z$ are integers. Adding, we get $(x - y) + (y - z)$ is also an integer, because $\mathbf{Z}$ is closed under sums. Hence $x - z$ is an integer, and this shows xRz, which shows R is transitive.

B) Show that the functions $\sin(2\pi x)$ and $\cos(2\pi x)$ are well-defined mod R.
Solution: This follows by the periodicity of sin and cos: Suppose xRx', so $x - x' = k \in \mathbf{Z}$. Then $x = x' + k$, so

$$\sin(2\pi x) = \sin(2\pi(x'+k)) = \sin(2\pi x'+2\pi k) = \sin(2\pi x')\cos(2\pi k)+\sin(2\pi k)\cos(2\pi x'),$$

using the addition formula for the sine. But $\cos(2\pi k) = 1$ and $\sin(2\pi k) = 0$ for all $k \in \mathbf{Z}$. Hence $\sin(2\pi x) = \sin(2\pi x')$. This shows sin is well-defined mod R. The proof for cos is similar.

C) Give a subset of $\mathbf{R}$ that contains a *unique* element from each of the equivalence classes for the relation R. (That is, your set should contain a's "hitting" all of the equivalence classes, but each one only once.
Solution: One such set is the interval $[0, 1) = \{x \in \mathbf{R} : 0 \leq x < 1\}$. If $x, x' \in [0, 1)$, then $|x - x'| < 1$, so $x - x'$ cannot be an integer, and x and x' are not related for this relation. On the other hand if x is any real number, then we can write $x = k + x'$ with $k = [x] \in \mathbf{Z}$ and $x' \in [0, 1)$. (k would be called the *greatest integer less than or equal to* x, and at least if $x > 0$, x' would be called the *fractional part* of x). This implies xRx', so the equivalence classes of the $x' \in [0, 1)$ account for all the equivalence classes.