Spring 2018 Math 406 Test II Review (with Solutions, still under construction)

Dr Holmes

April 25, 2021

The test review sheet is a homework assignment, due the Wednesday after the test. There may be some things on it that I will actually check over, notably things not covered on the exam.

Computational exercises which appear on the test should have closely related models here.

Similarly, you may expect that you will be ready for proofs on the test if you are ready to write the proofs of theorems whose proofs are assigned here and proofs which appear on the sample tests (if you have doubts about any of the proofs on the sample test, you can ask me whether they are likely to be covered).

The test is likely to have a certain number of computation questions, of which you can skip one, and a certain number of proof questions, of which you can skip one. I'm thinking of 5 of each as a first approximation, leaving 8 questions for you to complete.

1. Compute the unique solution to $x^5 \equiv_{337} 17$ (this will be a natural number less than 337).

   Solution: Compute the inverse of 5 in mod 336 arithmetic (336 because $x^k \equiv_{337} x^{k \mathtt{mod} 336}$ by Fermat's little theorem). This inverse is 336-67 = 269. The solution is then $17^{269} \mathtt{mod} 337 = 62$ (dont forget to switch back to mod 337 here). I left out the calculation of the inverse of 5 mod 336 using the extended Euclidean algorithm.

   Find a number with more than two distinct square roots in mod 135 arithmetic. Hint: factor the modulus to find an expression for m in the form $x^2 - y^2$ using a very familiar factoring formula.

Solution 135 = (for example) (5)(27) = (16+11)(16-11) = $16^2 - 11^2$, so $16^2 \equiv_{135} 11^2$, so $16^2 \texttt{mod} 135 = 121(!) = 11^2$, and 121 has at least 4 square roots, namely 11, 16, 135-16 = 119 and 135-11 = 124. Other factorizations of 135 would give different solutions to the problem: you could test comprehension by finding another one.

2. Prove that there is a unique kth root of a mod m when a is relatively prime to m and k is relatively prime to $\phi(m)$. This will need Euler-s Theorem on computing powers mod m and facts about reciprocals in modular arithmetic.

   Solution Don't forget that finding a solution and showing that it is the only solution are two different things (though in this case the calculations for the two parts are very similar).

   We are looking for x such that $x^k \equiv_m a$. The procedure is the same as in the previous problem, but in the abstract. Let n be the reciprocal of k in mod $\phi(m)$ arithmetic; this exists because k and $\phi(m)$ are relatively prime. Now $(a^n)^k = a^{nk} \equiv_m a^{nk \texttt{mod} \phi(m)}$ by Euler's theorem (this is where it is important that a is relatively prime to m) $= a^1 = a$. So $x = a^n$ is a solution.

   Now to prove uniqueness. Suppose that $x^k \equiv_m a$. We want to prove $x \equiv_m a^n$. $x = x^{kn \texttt{mod} \phi(m)}$ (Euler's theorem: x is obviously relatively prime to m because it has a power which is relatively prime to m) $\equiv_m (x^k)^n \equiv_m a^n$. so $x = a^n$ is the only solution.

   In your proof, I will be looking for the central calculations, and also for the remarks as to how the theorems you are allowed to use are applied.

3. RSA calculations: My RSA public key is $N = 221$, and my encryption exponent is 5.

   Compute the encrypted version of my favorite message 42.

   $42^5 \texttt{mod} 211 \equiv_{221} 9$

   Solution: 221=(13)(17) s $\phi(221) = 12 * 16 = 192$. We need to find the reciprocal of 5 in mod 192 arithmetic: this is 77, and 77 is my decryption exponent.

   Now compute my decryption exponent (since my key really isn't very secure). Some one sent me the message 36 over an open channel: decrypt it.

36^{77}mod221 = 134, which must be the original message. We check: 134^{5}mod221 realy is 36 as we expect.

4. Verify Carmichaelness and non-Carmichaelness of some numbers using Korselt's Criterion. You need to know the criterion.

   For this I refer you to exercise 19.3 in the book: these are not easy to generate.

   I'll be interested if you can figure out ways to search for moderate sized Carmichael numbers on the computer.

   Solution: I give solutions to selected example parts of 19.3.

   1105 = 5*13*17 is a Carmichael number because it has no square of a prime as a factor and 1105-1 = 1104 is divisible by each of 5-1, 13-1, 17-1. Your answer doesn't have to follow this exact format but it does need to reveal that you know what the criterion is.

   10659 = 3*11*17*19 is not a Carmichael number because 10658 is not divisible by 10, and 10658 would have to be divisible by all of 2, 10, 16 and 18 for 10659 toi be a Carmichael number.

   19747 = 7*7*13*31 is not a Carmichael number because it has a square of a prime as a factor.

5. Prove that there are no Carmichael numbers of the form pq where p and q are distinct primes. You may assume that you know that such a number would have to satisfy Korselt's Criterion, so your task is to show that it can't. (We did this in homework).

   Solution:

   omitted, because this question is on the Spring 2021 second exam.

6. Show that 497 is composite using the Rabin-Miller test. You may choose your starting number arbitrarily.

   Solution:

   $n = 497$

   I choose $a = 2$

   $n - 1 = 2^k q = 2^4 * 31$

   $2^q = 2^3 1 \equiv_{497} = 324$

$2^(2q) \equiv_{497} 324^2 \equiv_4 97109$

The first of these three numbers is not 1, and none of them are $496 \equiv_{497} -1$, so 497 is composite by the Rabin-Miller test.

Find a Rabin-Miller misleader for 25. I'd be interested if you could find examples of Rabin-Miller misleaders for other numbers: they do not seem to be common in practice!

7 is a misleader.

$24 = 2^3 * 3$ so $k = 3, q = 3$

$7^3 \equiv_{25} \equiv_{25} 18$

$7^{2*3} \equiv_{25} 18^2 \equiv_{25} 24 \equiv_{25} -1$

so we do not have proof that 25 is composite from this value of a. Of course, we know that 25 is composite, so this is an example of a misleader.

7. State the Rabin-Miller Test for compositeness [I will state it on the test]. Prove that it works (you may assume Fermat's Little Theorem and the Polynomial Root Theorem in your argument).

Solution: The proof on p 137 of your book is good. Of course it is a proof of the contrapositive (look at the logical relationship between theorem 19.2 and theorem 19.3. The proof also appears on p. 39 of my lecture notes, in a very similar form.

I'll write a statement of and argument for the compositeness test.

Suppose that n is an odd number and $n-1 = 2^k q$, with q odd (obviously odd n uniquely determines such a k and q).

We claim that if we can find a with $n \not| a$ such that $a^q \not\equiv_n 1$ and for each $i < k$, $a^{2^i q} \not\equiv_n -1$, then n is composite.

Suppose otherwise (that n is prime). Then $a^{2^k q}$ is equal to 1 (Fermat's little theorem and $2^k q = n - 1$), so there is a smallest nonnegative integer j such that $a^{2^j q} \equiv_n 1$. $j = 0$ is ruled out because $a^q \not\equiv_n 1$ is assumed. So $i = j - 1$ is a nonnegative integer. $a^{2^j q} \equiv_n 1$ is the square of $a^{2^i q}$, and by choice of j as minimal, $a^{2^i q} \not\equiv_n 1$. If n is prime the only square roots of 1 in mod n arithmetic are 1 and -1, so $a^{2^i q} \equiv_n -1$. Our i is less than k, so this contradicts our assumptions about n, so

our additional hypothesis that n is prime cannot hold: we have proved that n must be composite.

8. Prove that if $x \equiv_p y$, then $x^p \equiv_{p^2} y^p$ (this is a lemma I used in the opening stages of showing that the Rabin Miller test works 75 percent of the time).

   Solution: Suppose that $x \equiv_p y$, that is, $p|(x-y)$. Our aim is to show that $x^p \equiv_{p^2} y^p$, that is, that $p^2|(x^p - y^p)$.

   $x^p - y^p = (x-y)(x^{p-1} + x^{p-2}y + \ldots + xy^{p-2}y + y^{p-2})$. Observe that the second factor is the sum of p factors, each congruent to x^{p-1} mod p, since x and y are congruent mod p, so the second factor is divisible by p. The first factor is divisible by p by hypothesis. Thus the difference is divisible by p^2, which is what we needed to show.

9. How many generators (primitive roots) are there in mod 31 arithmetic? Find one of them.

   Hint: pick a residue and compute certain powers of that residue to check whether it is a generator.

   Solution: There are $\phi(30) = \phi(2)\phi(3)\phi(5) = 1 * 2 * 4 = 8$ generators.

   A generator g will satisfy $g^{15} \not\equiv_{31} 1$, $g^{15} \not\equiv_{31} 1$, and $g^6 \not\equiv_{31} 1$: the exponents are each obtained by dividing 30 by one of its prime factors.

   2^10 is congruent to 1, reject 2

   3^6 is congruent to 16, 3^{10} is congruent to 25, 3^{15} is congruent to 16. 3 is a generator.

   In the compass of a homework problem (but not a test question), go ahead and determine the orders of all residues mod 31 and check that you have the number of elements of each order that you expect.

10. Explain how to find a generator for a safe prime (a prime p such that $p = 2q + 1$ where q is prime). Why is it computationally hard to find a generator for an arbitrary large prime p?

    The only prime factors of $p-1 = 2q$ are 2 and q. So the non-generators will be either of order 1 (this exclude 1) order 2 (this excludes -1) or order q (excluding numbers for which $a^q \equiv_p 1$). There will be $\phi(2q) = q - 1$ generators, and one finds them by randomly choosing a number in $[2, p-2]$ (choice of interval excludes 1 and -1) and accepting it if

$a^q \not\equiv_p 1$ (the only other alternative is $a^q \equiv_p -1$). The chance of getting a generator is fifty percent.

The reason the problem of finding a generator is hard in general is that one needs to factor $p-1$ to find a generator efficiently. Factoring large numbers is hard.

11. Prove that there are infinitely many primes of the form $4n+1$ (notice that this requires one of the parts of the QRT). If I asked this question, I might provide the easier proof that there are infinitely many primes of the form $4n+3$ as an alternative for partial credit.

    Solution:

    The proof of the main theorem is on pp. 152-3 in your book. The proof of the alternative theorem is on p. 86. Both are also found in very similar forms in the lecture notes.

12. Determine whether 137 is a quadratric residue mod 337, using the Generalized QRT. Annotate all steps carefully so that I can verify correctness of your work.

    $\left(\frac{137}{337}\right) = \left(\frac{337}{137}\right)$ (flip without a minus sign because 337 mod 4 is 1) $= \left(\frac{63}{137}\right) = \left(\frac{137}{63}\right)$(flip without minus sign because 137 mod 4 is 1) $= \left(\frac{11}{63}\right) = -\left(\frac{63}{11}\right)$ (63 and 11 both have remainder 3 on division by 4, thus the minus sign) $= -\left(\frac{8}{11}\right) = -\left(\frac{2^3}{11}\right) = -\left(\frac{2^2}{11}\right)\left(\frac{2}{11}\right) = -(1)(-1)$ (2^2 is of course a QR, 2 is an NR mod 11 by second part of QRT since 11 mod 4 is 3)$= -1$. 137 is an NR mod 337.

    Most of the credit is not for the one-bit answer, but for careful description of the process.

13. Verify that if $p = 4k+3$ is a prime, and a is a quadratic residue mod p, then $x = a^{\frac{p+1}{4}}$ is a solution to $x^2 \equiv_p a$. Compute a square root using this theorem: for example, compute the square root of 2915 in mod 4703 arithmetic. (OK, you'll need Sage for this one. But I can generate an example you can actually do on a TI89 relatively easily).

    $(a^{\frac{p+1}{4}})^2 = a^{\frac{p+1}{2}} = a^{\frac{p-1}{2}+1} = (a^{\frac{p-1}{2}})(a) \equiv_p \left(\frac{a}{p}\right) a = a$ because a is assumed to be a QR.

In calculations for a problem like this, do not use fractional exponents unless you know them to be integers. In this case, all the fractions we write actually come out even.

14. Prove that the product of two non-quadratic residues mod p is a quadratic residue mod p.

    The easy way to prove this, which my instructions do not rule out, is to use Euler's Criterion.

    Suppose that x and y are NRs mod p. Then $\left(\frac{xy}{p}\right) \equiv_p (xy)^{\frac{p-1}{2}} = x^{\frac{p-1}{2}} y^{\frac{p-1}{2}} \equiv_p \left(\frac{x}{p}\right)\left(\frac{y}{p}\right) = (-1)(-1) = 1$.

15. Exhibit two squares which add to 1109, using the technique on page 187 of the book. A photocopy of page 187 will be attached to your test.

    I give you for free the information that $354^2 + 1^2$ is divisible by 1109.

    $354^2 + 1^2 = (113)(109)$

    $A = 354; B = 1; M = 113$

    $u = 354 mod 113 = 15; v = 1 mod 113 = 1$

    new A is $\frac{(134)(15)-1}{113} = 47$

    new B is $\frac{134-15}{113} = 3$

    $47^2 + 3^2 = 2218 = (2)(1109)$

    new M is 2

    new u is $47 mod 2 = 1$; new v is $3 mod 2 = 1$

    next A is $\frac{47(1)+3(1)}{2)} = 25$

    next B is $\frac{47(1)-3(1)}{2} = 22$

    $25^2 + 22^2 = 1109$

    This example is nice in that it is short. It is too simple in that one never needs to cut down the absolute value of a u or v.

16. an additional example: compute the sum of the divisors of $5965164 = 2^2 3^5 1719^2$

    Solution: $(1+2+4)(1+3+3^2+3^3+3^4+3^5)(1+17)(1+19+19^2) = (\frac{2^3-1}{2-1})(\frac{3^6-1}{3-1})(\frac{17^2-1}{17-1})(\frac{19^3-1}{19-1}) = 17474184$

    In such a question, I would supply the factorization.