Solution

Math 406, Spring 2018, Test II

Dr. Holmes

4/20/2018

This exam will begin at 10:30 am and end at 11:45 am, officially. You will actually get a five minute warning at 11:45.

There are five computational questions (1-5) and four proof questions (6-9) on the test. You may safely skip one proof question and one computational question; class performance may cause me to make further adjustments. If you work on all problems, you do not need to tell me which one to omit: your best work will count.

There is an entirely optional question 10, which you may choose to do as a proof question. This was a question on Test I: good performance on question 10 will count on this test and may improve your grade on Test I as well. Question 10 if you do it will count as one of your four proof questions, and the usual remark about your best work counting applies.

You may use your writing instrument, your test paper, and any calculator. I will try to have scratch paper available if you need it.

1. Find the unique solution (up to congruence mod 137) to the equation $x^{21} \equiv_{137} 2$.

find 21^{-1} mod 136

136	1	0	
21	0	1	
10	1	-6	6
	-1	~~21~~ $\boxed{13}$	2

$(x^{21})^{13} \equiv_{137} 2^{13} \equiv_{137} \boxed{109}$

✓

2. Compute the sum of the divisors of 31,212 $= 2^2 * 3^3 * 17^2$. Hint: use the fact that "sum of the divisors" is a multiplicative function.

$(1+2+2^2)(1+3+9+27)(1+17+17^2)$

$\boxed{5040}$

85960

3. Verify that 7 is a Rabin-Miller misleader for $n = 25$ (do the calculations and point out briefly why they don't give the information you need to show that 25 is composite) Then use the Rabin-Miller test to verify that 25 is composite; almost any a other than 7 will do (yawn, I know): the point is to show that you can execute the test, not that it is hard to see that 25 is composite. I do seem to recall that there is another misleader, but I doubt you will run into it.

$n = 25 \quad n-1 = 24 = 2^3 \cdot 3$

$7^3 = 343 \equiv_{25} 18$

$18^2 \bmod 25 = 24 \equiv -1$

and $2 < 3$, so 7 is a misleader.

It doesn't tell us that 25 is composite!

~~lets~~ try $a = 2$

$2^3 = 8$

$8^2 \equiv_{25} 14$

neither is 24, 25 is composite

$14^2 \equiv_{25} 21 \; (\not\equiv_{25} 1$

this is a Fermat witness

so definitely a Rabin Miller witness.

4. How many primitive roots (generators) are there in mod 23 arithmetic? Find one, and verify that it is a generator. You can do the verification by listing all powers, or by giving the correct short list of powers of the generator which confirms that it is a generator.

There are $\phi(22) = \phi(2)\phi(11) = 10$ generators (a lot, this is a safe prime!)

$2^{11} \equiv 1$ not a generator

$\boxed{5^{11} \equiv 22 \quad 5 \text{ is a generator}}$

5. Use the algorithm described on the attached page to determine two numbers whose squares add to 281.

   I give you for free the information that $228^2 + 1^2$ is a multiple of 281.

   I also supply the information that you *do* need to pay attention to the signs of u and v in these calculations if you have occasion to cut them down in absolute value. But I believe this does not happen in this example.

$A = 228 \quad B = 1$

$228^2 + 1^2 = \overset{m}{(185)}(281)$

$u \quad \checkmark$

$43 \quad 1$

$\dfrac{228 \cdot 43 + 1}{185} \qquad \dfrac{228 - 43}{185}$

$53^2 + 1^2 = 2810 = \overset{m}{(10)}(281)$

u

$3 \quad 1$

$\dfrac{53 \cdot 3 + 1}{10} \qquad \dfrac{53 - 3}{10}$

$\boxed{16^2 + 5^2 = 281}$

6. Prove that for any modulus m (it does not have to be prime), number a relatively prime to m, and number k relatively prime to $\phi(m)$, there is a unique solution to the equation $x^k \equiv_m a$. Your work will show how to compute a solution, and then also show that the solution you find is the only solution.

Let $\gcd(a, m) = 1$, and let $\gcd(k, \phi(m)) = 1$.

Since $\gcd(k, \phi(m)) = 1$, there is l s.t.

$$kl \equiv_{\phi(m)} 1$$

Let $x = a^l$.

$$(a^l)^k = a^{lk} \equiv_m a^{lk \bmod \phi(m)} = a$$

Euler's Thm + $\gcd(a,m) = 1$

So $x = a^l$ is a solution,

Now suppose $x^k = a$. Our goal is to show $x = a^l$.

$$a^l = (x^k)^l = x^{kl \bmod \phi(m)} = x!$$

7. Prove that $2^{p-1}(2^p - 1)$ is a perfect number if $2^p - 1$ is prime. You do not need to prove the converse result that all even perfect numbers are of this form. Hint: you may find some use for the formula for the sum of a finite geometric series.

The factors of $2^{p-1}(2^p-1)$ are

powers of 2 $1, 2, 4, \ldots 2^{p-1}$ which add up to $\boxed{2^p - 1}$

and powers of 2 times (2^p-1) which add up to $(\cancel{2^p - 1})(2^p-1)$ (2^p-1)

a prime - important, since there would be more divisors

added together, the sum of all the divisors is $(\cancel{2^p-1}+1)(2^p-1)$ $= 2^p(2^p-1)$

~~or~~ $2^p(2^p-1)$. Take out the improper

divisor $2^{p-1}(2^p-1)$ and you get $2^{p-1}(2^p-1)$ as

the sum of the proper divisors,

~~thus the~~

the number is perfect.

8. Prove the Rabin-Miller test for compositeness. This is the assertion that if n is an odd number, with $n-1 = 2^k q$ where q is odd, and there is an a not divisible by n such that $a^q \not\equiv_n 1$ and for no $i < k$ do we have $a^{2^i q} = -1$, then n is composite. You may use Fermat's Little Theorem and the Polynomial Root Theorem for prime moduli.

Suppose that n is an odd number, $n-1 = 2^k q$ where q is odd (clearly there are unique such k and q), and $a^q \not\equiv_n 1$ and for no $i<k$ do we have $a^{2^i q} \equiv_n -1$.

Suppose for the sake of a contradiction that n is prime.

Then $a^{2^k q} = a^{n-1} \equiv_n 1$ by Fermat's Little Theorem.

Thus there is a first j such that $a^{2^j q} \equiv_n 1$ and $j \leq k$.

$j \neq 1$ by hypothesis $(a^q \not\equiv_n 1)$

so $0 \leq j-1 < k$ and $\left(a^{2^{j-1} q}\right) \not\equiv_n 1$

and $\left(a^{2^{j-1} q}\right)^2 = a^{2^j q} \equiv_n 1$

so by PRT (n being prime) $a^{2^{j-1} q} \equiv_n -1$

which is a <u>contradiction</u> to our assumptions.

9. Prove that there are infinitely many primes of the form $4n+1$. You will need to use one of the cases of the Quadratic Reciprocity Theorem in your proof. If you cannot do this, you may earn significant partial credit by proving the easier theorem that there are infinitely many primes of the form $4n+3$. If you prove both, some extra credit is possible.

Suppose that there are finitely many prime $p_1 \cdots p_n$ of the form $4n+1$.

Consider $A = (2p_1 \cdots p_n)^2 + 1$

This must have a prime factor q which cannot be any of $2, p_1, \ldots, p_n$. Notice that -1 is a quadratic residue mod q. But then q is of the form $4n+1$, contradiction, by 2nd part of QRT

$\left(\frac{-1}{p}\right) = 1$ iff p is of form $4n+1$ if p is odd

The other part:

Suppose $p_1, \ldots, p_n$ are all the primes of the form $4n+3$.

Consider $A = p_1 p_2 \cdots p_n + 2$ and $B = p_1 \cdots p_n + 4$.

one of these is of the form $4n+3$, and so has a prime factor of the form $4n+3$ which cannot be any of the p_i's.

10. (completely optional) Prove that in any primitive Pythagorean triple $a^2 + b^2 = c^2$, c is not divisible by 7. (Success on this question may improve your grade on Test I as well as counting here). You may earn additional credit (as on the original question) by describing the patterns which can occur with values of $a \bmod 7$ and $b \bmod 7$ in PPTs.

a ~~0 1 2 3 4 5~~

0^2	0
1^2	1
2^2	4
3^2	2
4^2	2
5^2	4
6^2	1

a^2

b^2	0	1	2	4
0	~~0~~	1	2	4
1	1	2	~~3~~	~~5~~
2	2	~~3~~	4	~~6~~
4	4	~~5~~	~~6~~	1

c^2 must also be 0, 1, 2, 4 mod 7

0 is x'ed out bc it is a PPT ($a = b = 0$ is ruled out)

So we can see that $c \neq 0$

if ~~both a, b ≠ 0~~ ~~...~~ one of a, b is not 0

$\boxed{\text{Further we can see that either one of } a, b \text{ is divisible by 7 or } a \equiv_7 b.}$ add'l credit

Descent Procedure

$p = 881$	p any prime $\equiv 1 \pmod 4$
Write $387^2 + 1^2 = 170 \cdot 881$ with $170 < 881$	Write $A^2 + B^2 = Mp$ with $M < p$
Choose numbers with $47 \equiv 387 \pmod{170}$ $1 \equiv 1 \pmod{170}$ $-\frac{170}{2} \leq 47, 1 \leq \frac{170}{2}$	Choose numbers u and v with $u \equiv A \pmod M$ $v \equiv B \pmod M$ $-\frac{1}{2}M \leq u, v \leq \frac{1}{2}M$
Observe that $47^2 + 1^2 \equiv 387^2 + 1^2$ $\equiv 0 \pmod{170}$	Observe that $u^2 + v^2 \equiv A^2 + B^2$ $\equiv 0 \pmod M$
So we can write $47^2 + 1^2 = 170 \cdot 13$ $387^2 + 1^2 = 170 \cdot 881$	So we can write $u^2 + v^2 = Mr$ $A^2 + B^2 = Mp$ (for some $1 \leq r < M$)
Multiply to get $(47^2 + 1^2)(387^2 + 1^2)$ $= 170^2 \cdot 13 \cdot 881$	Multiply to get $(u^2 + v^2)(A^2 + B^2) = M^2 rp$
Use the identity $(u^2 + v^2)(A^2 + B^2) = (uA + vB)^2 + (vA - uB)^2$.	
$(47 \cdot 387 + 1 \cdot 1)^2 + (1 \cdot 387 - 47 \cdot 1)^2$ $= 170^2 \cdot 13 \cdot 881$ $\underbrace{18190^2 + 340^2}_{\text{each divisible by } 170} = 170^2 \cdot 13 \cdot 881$	$\underbrace{(uA + vB)^2 + (vA - uB)^2}_{\text{each divisible by } M} = M^2 rp$
Divide by 170^2. $\left(\frac{18190}{170}\right)^2 + \left(\frac{340}{170}\right)^2 = 13 \cdot 881$ $107^2 + 2^2 = 13 \cdot 881$ This gives a smaller multiple of 881 written as a sum of two squares.	Divide by M^2. $\left(\frac{uA + vB}{M}\right)^2 + \left(\frac{vA - uB}{M}\right)^2 = rp$ This gives a smaller multiple of p written as a sum of two squares.
Repeat the process until p itself is written as a sum of two squares.	