Math 287, Spring 2022, Test II

Dr Holmes

April 6, 2022

This exam will be given from 1030-1145 on Thursday April 7.

You are allowed your test paper, your writing instrument, and a non-graphing calculator.

1. Define $a_1 = 6; a_2 = 20; a_{k+2} = 6a_{k+1} - 8a_k$.

   Compute the terms of this sequence up to a_6.

   Prove by strong induction that $a_n = 2^n + 4^n$ for each natural number n.

$a_1 = 6 \quad a_2 = 20$

$a_3 = 6\cdot 20 - 8\cdot 6 = 72$

$a_4 = 6\cdot 72 - 8\cdot 20 = 272$

$a_5 = 6\cdot 272 - 8\cdot 72 = 1056$

$a_6 = 6\cdot 1056 - 8\cdot 272 = 4160$

~~n=0 ...~~

$n=1 \quad 2^1 + 4^1 = 6 = a_1$

$n=2 \quad 2^2 + 4^2 = 4 + 16 = 20$

Suppose that for all $m \leq k$ $(k \geq 2)$ $a_k = 2^k + 4^k$.

Show that $a_{k+1} = 2^{k+1} + 4^{k+1}$.

$$a_{k+1} = 6\cdot a_k - 8\cdot a_{k-1} \underset{\text{ind hyp}}{=} 6(4^k + 2^k) - 8(4^{k-1} + 2^{k-1})$$

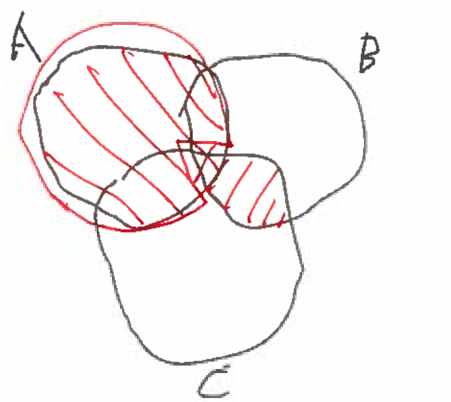
$$= 24(4^{k-1}) + 12(2^{k-1}) - (8)4^{k-1} - (8)2^{k-1}$$

$$= 16\cdot 4^{k-1} - 4\cdot 2^{k-1}$$

$$= 4^{k+1} - 2^{k+1}.$$

2. Give a Venn diagram demonstration of the identity $A - (B \cap C) = A - B \cup A - C$.

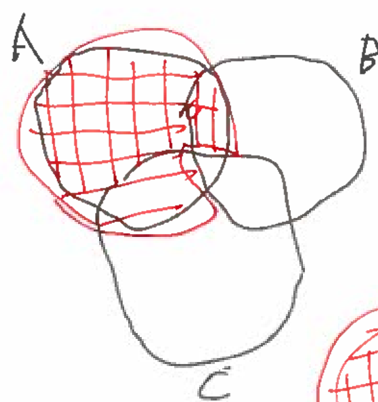
   You should shade sets of interest informatively in each of the two pictures, provide a key to the shadings, and clearly outline the set which is the result of the computation.



$A-(B\cap C)$

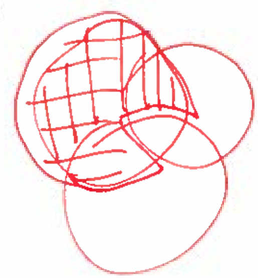
$B \cap C$

A



$A-B$

$\cap$



$A-B$

$A-C$

same set picked on both sides

3. Do one of the two proofs. If you do both, the best one will count; if you do well on both extra credit is possible.

   (a) Prove that the relation $x \equiv_n y$ is an equivalence relation

$X \equiv_n y$ means $n \mid (x-y)$

reflexive: show that $X \equiv_n x$

This means $n \mid (x-x)$ and it is true that $n \mid 0$ for any n.

symmetric: show that if $x \equiv_n y$ then $y \equiv_n x$.

If $x \equiv_n y$ then $n \mid (x-y)$ so $x-y = kn$ for some $k \in \mathbb{Z}$

So $y-x = (-k)(n)$ so $n \mid (y-x)$ so $y \equiv_n x$.

transitive suppose $X \equiv_n y$ and $y \equiv_n z$.

This means $n \mid (x-y)$ and $n \mid (y-z)$ i.e. $\exists k, l \in \mathbb{Z}$

$kn = x-y$ and $ln = y-z$. then $(k+l)n = (x-y)+(y-z)$
$= x-z$

so $n \mid (x-z)$ so $X \equiv_n z$.

(b) Prove that if $a \equiv_n a'$ and $b \equiv_n b'$, then $ab \equiv_n a'b'$.

$a \equiv_n a' \Rightarrow$ ~~...~~ $a' = a + kn$ for some $k \in \mathbb{Z}$

$b \equiv_n b' \rightarrow$ $b' = b + ln$ for some $l \in \mathbb{Z}$

then ~~(a+kn)~~ $a'b' = (a+kn)(b+ln) =$

$ab + aln + bkn + kln^2$

so $a'b' - ab = (al + bk + kln)n$

is divisible by n, ~~as~~ so $ab \equiv_n a'b'$.

4. Construct addition and multiplication tables for mod 7 arithmetic, and make a table of multiplicative inverses.

·	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

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

x	x^{-1}
0	—
1	1
2	4
3	5
4	2
5	3
6	1

5. Prove Euclid's Lemma: if p is prime and $p|ab$ then either $p|a$ or $p|b$.

The proof depends on the extended Euclidean algorithm theorem, which I remind you says that for any a, b not both equal to zero there are integers x, y such that $ax + by = \gcd(a, b)$.

If $p|a$ we are done.

Suppose $p \nmid a$. Then $\gcd(p, a) = 1$ so

$\exists\, x, y \in \mathbb{Z}$, $ax + py = \gcd(a, p) = 1$ (p is prime!)

So $b = \cancel{bax+}\ 1b = axb + pyb$ which is divisible by p.

axb: divisible by p because ab is

pyb: divisible by p by inspection

In either case, one of a, b is divisible by p.

6. Each of the parts in this problem provides information for the next one.

(a) Find integers x, y such that $137x + 15y = 1$ using the extended Euclidean algorithm (my table format).

r	x	y	q
137	1	0	
15	0	1	
2	1	-9	9
1	-7	64	7

$(-7)(137) + (15)(64) = 1$ ✓

(b) Compute $15^{-1} \mathtt{mod} 137$.

64 from just above.

(c) Solve the equation $15x \equiv_{137} 16$ for x.

$15x \equiv_{137} 16$

$(64)(15)x \equiv_{137} (64)(16)$

1024

$1024 - 7(137) = \boxed{65}$

7. Compute $23^{72} \bmod 100$ using the method of repeated squaring. Show all work.

72	$\boxed{21}$
36	61
18	69
9	63
4	41
2	29
1	23

8. Simplification of modular exponentiation.

(a) Use Fermat's Little Theorem to simplify the calculation of $2^{927}\mathtt{mod}23$

$$2^{927} \equiv_{23} 2^{927 \bmod 22} = 2^3 = \boxed{8}$$

(b) Use Euler's Theorem to simplify the computation of $5^{1282}\mathtt{mod}55$ (notice that 55 is of the form pq with p and q prime).

$$55 = (5)(11)$$

$$\phi(55) = (4)(10) = 40$$

$$5^{1282} \bmod 55 = 5^{1282 \bmod 40} \bmod 55 = 5^2 = \boxed{25}$$

9. My public key has $N = 55, r = 3$.

   Encrypt the message 42 to me.

   My secret, which you can't possibly guess, is that $N = (5)(11)$.

   Determine my decryption exponent s.

   Carry out the calculation I will do to decrypt your message.

   (The numbers here are wonderfully small; of course the cryptographic security is zip!)

$42^3 = 74088 - (1347)(55) = \boxed{3}$

$42^3 \bmod 55 = 3$

$\phi(N) = 4 \cdot 10 = 40$

$s = r^{-1} \bmod 40$

40	1	0	
3	0	1	
1	1	-13	13

$40 - 13 = 27$

decryption: $3^{27} \bmod 55$

27	$38^2 \cdot 3 = 4332 - (78)(55) = 42$
13	$14^2 \cdot 3 = 588 - 10 \cdot 55 = 38$
6	$729 - (13)(55) = 14$
3	27
1	3