Math 187 Test IV, Spring 2012

Dr. Holmes

May 1, 2012

The exam will begin at 140 pm and end at 235 pm. You may use your writing instrument, your non-graphing scientific calculator, and your test paper. If you require scratch paper I will have some.
1. Find a solution to the system of equations

\[ x \equiv 6 \mod 13 \]
\[ x \equiv 9 \mod 19 \]

Find another solution (hint: what is the appropriate modulus?)

Two strategies are possible.

One starts with \( x = 6 + 13k \) for some \( k \). The other starts with \( x = 9 + 19k \) for some \( k \).

First strategy:
\[ x = 6 + 13k = 9 \mod 19 \]

so
\[ 13k = 3 \mod 19 \]

to solve this we need to find the reciprocal of 13 mod 19.

\[
\begin{array}{cccc}
19 & 1 & 0 \\
13 & 0 & 1 \\
6 & 1 & -1 & 1 \\
1 & -2 & 3 & 2 \\
\end{array}
\]

From this we see that \((-2)19 + 3(13) = 1\) from which we see that the reciprocal of 13 mod 19 is 3, and the reciprocal of 19 mod 13 is \(-2\), or equivalently in mod 13, \(13 - 2 = 11\).

Thus we get \( k = 9 \mod 19 \) (multiplying both sides by 3) so \( x = 6 + (13)(9) = 123 \).

The appropriate modulus is \(13)(19) = 247\). Another solution would be for example \(123 + 247 = 370\).

Second strategy:
\[ x = 9 + 19k = 6 \mod 13 \]
\[ 19k = -3 = 10 \mod 13 \]

we know from above that the multiplicative inverse of 19 mod 13 is 10.

\[ k = 110 \]

so \( x = 9 + (19)(110) = 2099 \)

which is a solution. Another one would be \(2099 \mod 247 = 123\).
2. Necklace counting

(a) A closed necklace with no clasp has 11 beads of 4 colors. How many such necklaces are possible?

4 monochromatic. $4^{11} - 4$ closed nonmonochromatic necklaces: an open nonmonochromatic necklace corresponds to 11 of these, so $4 + \frac{4^{11} - 4}{11} = 381304$ is the number of open necklaces.

I gave 7 points if you just wrote $\frac{4^{11} - 4}{11}$; this is a significant conceptual error.

(b) (extra credit) A closed necklace has 15 beads of 3 colors. How many such necklaces are possible?

The extra credit part could add up to 2 points to a successful part a: I also used it to completely replace a missing or unsatisfactory part a (in which case there were no EC points).

3 monochromatic necklaces.

$3^3 - 3 = 24$ closed necklaces with a repeating pattern of length 3. Each open necklace with such a pattern corresponds to 3 of these, so there are 8 open necklaces with a pattern of length 2.

$3^5 - 3 = 240$ closed necklaces with a repeating pattern of length 5. Each open necklace with such a pattern corresponds to 5 of these, so there are $\frac{240}{5} = 48$ open necklaces with a pattern of length 5.

$3^{15} - (3^5 - 3) - (3^5 - 3) - 3 = 14348640$ closed necklaces with a repeating pattern of length 15. Each open necklace with such a pattern corresponds to 15 of these, so there are $\frac{14348640}{15} = 956576$ of these open necklaces.

Now the total number of open necklaces is 956576 (adding up the numbers of open necklaces found above).
3. Modular exponentiation

(a) Compute $7^{435627650} \mod 13$ Hint: Fermat’s little theorem makes this a snap.

$435627650 \mod 12 = 2$ (no credit for mod 13 here). So $7^2 \mod 13 = 10$ is the answer we seek.

(b) Compute $11^{1024} \mod 100$ (a different set of tricks makes this straightforward)

Calculations are in mod 100:

- $11^2 = 21$
- $11^4 = 21^2 = 41$
- $11^8 = 41^2 = 81$
- $11^{16} = 81^2 = 61$
- $11^{32} = 61^2 = 21$ (repeats from here on)
- $11^{64} = 41$
- $11^{128} = 81$
- $11^{256} = 61$
- $11^{512} = 21$
- $11^{1024} = 41$ which is the answer.
4. Degree sequences

(a) For each of the two following degree sequences, either draw a graph with that degree sequence or give a brief explanation as to why there cannot be one.

i. 4, 4, 3, 2, 2, 1

![Graph with degree sequence 4, 4, 3, 2, 2, 1]

There are other solutions

ii. 4, 3, 3, 2, 2, 1
impossible because a finite graph cannot have an odd number of vertices of odd degree.

(b) Show me two nonisomorphic graphs with the degree sequence 2, 2, 2, 2, 2, 2

![Two nonisomorphic graphs with degree sequence 2, 2, 2, 2, 2, 2]
5. One of the two pictured graphs has an Eulerian trail. One doesn’t. Explain why the one that doesn’t, doesn’t, and give an Eulerian trail for the other in the form of a list of vertices visited in order.

\[ \text{a}, \ b, \ d, \ e, \ b, \ c, \ e, \ f, \ c, \ a \]

If vertices of odd degree, no Eulerian trail.
6. Prove using the Pigeonhole Principle that if I choose 10 points in a 3 × 3 square, two of them will be at distance ≤ \(\sqrt{2}\) from each other. Be sure to state the counting facts you use.

The 3 by 3 square divides into 9 1 by 1 squares. If we put 10 points into 9 boxes, at least two must be in the same box. Within a 1 by 1 box, the farthest apart that two points can be is \(\sqrt{2}\). So the two points in the same box are at distance \(\leq \sqrt{2}\) from each other.
7. RSA problem

Your RSA key \( N = pq \) is 55 and your encryption exponent \( r \) is 3.

(a) Find your decryption exponent (Hint: it is the reciprocal of 3 in a certain modulus). Show all work.

\( p = 5; q = 11 \). The modulus for exponents is \((p - 1)(q - 1) = 4(10) = 40\).

The encryption exponent is the reciprocal of 3 in mod 40 arithmetic.

\[
\begin{array}{ccc}
40 & 1 & 0 \\
3 & 0 & 1 \\
1 & 1 & -13 & 13 \\
\end{array}
\]

The reciprocal is \(-13 = 27 \mod 40\).

(b) Decode the message 17. Show all work.

\[17^{27} \mod 55 = 7^2 \cdot 17 = 8\]
\[17^{13} \mod 55 = 49^2 (17) = 7\]
\[17^6 \mod 55 = 18^2 = 49\]
\[17^3 \mod 55 = (17^2)(17) = 18\]
\[17^1 \mod 55 = 17\]

The message was 8.
8. Factoring magic

(a) Prove this theorem: if $p$ is a prime, and $p|ab$, then either $p|a$ or $p|b$.

Your proof should not mention prime factorizations: it is the basis for the proof of the uniqueness of prime factorizations! It should use the basic theorem about greatest common divisors and the definition of divisibility. (another part on the next page)

Assume $p|ab$.

Our goal is to show "$p|a$ or $p|b$".

Suppose $p \nmid a$. Then our goal is to show $p|b$.

Because $p \nmid a$, we have $\gcd(p, a) = 1$, so there are integers $x, y$ such that $px + ay = 1$, so $b = b \cdot 1 = b(px + ay) = bpx + bay$. $bpx$ is obviously divisible by $p$. $bay$ is divisible by $p$ because $ba = ab$ is divisible by $p$. So $b = b \cdot 1 = b(px + ay) = bpx + bay$ is divisible by $p$. That is, $b|p$, which is what we needed to prove.
(b) Use the theorem proved in part a to prove this theorem: if 3|x and 7|x then 21|x.

I want you to use the theorem of the first part – nothing about prime factorizations. Further, you should explicitly use the definition of divisibility: this will help you see how to use the theorem of part a!

Suppose 3|x and 7|x. Because 3|x there is an integer k such that x = 3k. Since 7|x we have 7|3k, so either 7|3 or 7|k by the theorem of part a. 7|3 is false, so 7|k must be true, that is, there is m such that k = 7m. But then x = 3k = 3(7m) = (3 \cdot 7)m = 21m so x is divisible by 21.