More Midterm Review

Monday, November 2

Number Theory

1. True or false: there exist integers x and y such that $13x + 41y = 7$.

   True by Bezout's Theorem since 13 and 41 are relatively prime.

2. True or false: there exist integers x and y such that $15x + 21y = 7$.

   False since $\gcd(15, 21) = 3$ but $3 \nmid 7$.

3. Prove or give a counterexample: if $d|a$ and $d|b$ then $d| \gcd(a, b)$.

   True: Say $a = dj$ and $b = dk$. We know that there exist x and y such that $ax + by = \gcd(a, b)$, but this means that $(dj)x + (dk)y = \gcd(a, b)$, and so $d(jx + ky) = \gcd(a, b)$. Thus any common divisor of a and b divides the greatest common divisor.

4. Prove that if n is odd then $n^2 \equiv 1 \pmod 8$.

   n is either 1, 3, 5, or 7 mod 8, so we just have to check that $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod 8$.

5. What is 11^{122} mod 7?

   By Fermat's Little Theorem, $11^6 \equiv 1 \pmod 7$. Thus $11^{122} \equiv 11^{6 \cdot 20} \cdot 11^2 \equiv 1 \cdot 2 \equiv 2 \pmod 7$.

Cryptography

1. If we encrypt a number with the scheme $p \mapsto p^{11} \pmod{35}$, then what is the decryption exponent?

   $35 = 7 \cdot 5$, so we want to find the multiplicative inverse of 11 mod $(7 - 1)(5 - 1) = 24$. As it turns out 11 is its own inverse since $11^2 = 121 \equiv 1 \pmod{24}$, so the decryption exponent is the same as the encryption exponent (not a very secure system!).

Induction

1. Given: if p is prime and $p|ab$ then $p|a$ or $p|b$. Prove: if p is prime and $p|a_1 a_2 \cdots a_n$ then $p|a_i$ for some i.

   Proof by induction: The case $n = 2$ is already given.

   Then suppose it holds for n. If $p|(a_1 \cdots a_n)a_{n+1}$ then either $p|a_1 \cdots a_n$ or $p|a_{n+1}$. In the latter case, we are done. In the former, the inductive hypothesis implies that $p|a_i$ for some i between 1 and n. Either way, $p|a_i$ for some i between 1 and $n + 1$, so the proof by induction is complete.

2. Prove that consecutive Fibonacci numbers are relatively prime.

   Base case: $f_0 = 0$ and $f_1 = 1$ are relatively prime.

   Inductive step: Suppose $\gcd(f_{n-1}, f_n) = 1$. Then $\gcd(f_n, f_{n+1}) = \gcd(f_n, f_n + f_{n-1}) = \gcd(f_n, f_{n-1}) = 1$. This completes the proof by induction.

Counting

1. How many ways are there to buy 7 fruit if your have 10 choices of fruit?

   Stars and bars: there are 9 "bars" dividing the fruit and 7 stars, so the number of options is $\binom{16}{7}$.

2. What if you want to buy at least one apple and exactly one pear?

   Buy an apple and a pear. Now you want to buy 5 fruit and have 9 types to choose from (removing the pears), so there are 5 stars and 8 bars, giving you $\binom{13}{5}$ options.

Probability

1. What is the chance that a random permutation of the string "COMBINATORICS" will be "MANICROBOTICS"?

   There are $13!/(2!)^3$ distinct ways to rearrange the letters, so the chance of making the desired string is $8/13!$.

2. Urn A has 3 red balls and 1 green ball. Urn B has 2 red balls and 3 green balls. You draw a ball from a random urn and win a prize if you correctly guess which urn you drew the ball from. Which color ball would you rather draw?

   If you draw a red ball then the relative odds are $3/4 : 2/5 = 15 : 8$. If you draw a green ball then the relative odds are $1/4 : 3/5 = 5 : 12$. The odds in the second case are more lopsided, so drawing a green ball would give you the better chance of guessing correctly.

3. A loaded six-sided die rolls the number n with probability $n/21$ for $n = 1, 2, \ldots, 6$. If you roll such a die three times, what is the probability that the sum of the three rolls will be 6?

   The two ways to roll a total of 6 are $1 + 1 + 4$ and $1 + 2 + 3$. Accounting for the number of ways to rearrange these rolls, the probability is then $3 \cdot (1/21)^2 \cdot (4/21) + 6 \cdot (1/21) \cdot (2/21) \cdot (3/21) = 48/21^3$.