ECE 312, Discrete Mathematics

Final Exam Solution

Rutgers University

Date and time: April 11, 2018, 3:20 to 4:40 pm.

Instructions: The exam is **closed book** and consists of **6 problems**. Make sure you write your name and NetID on the paper. **Show all your work**, you will not receive full credit if your answer lacks the necessary explanations. The last two pages of the exam can be used as scratch paper. Cheating $\implies 0$.

Problem I: *(15 points + 5 bonus points)* We want to prove the following theorem.

Theorem 1 *If a, b, and c are positive integers such that $\gcd(a, b) = 1$ and $a|bc$, then $a|c$.*

1. *(5 points)* Give an example explaining the result above.
2. *(5 points)* Would the result above still be true if we remove the condition that $\gcd(a, b) = 1$? If not provide a counterexample.
3. *(5 points)* Use Bézout's theorem to prove the theorem above.

Solution:

1. *(5 points)* Let $a = 3$, $b = 2$, $c = 6$ be three positive integers satisfying $\gcd(a, b) = 1$ and $a = 3$ divides $bc = 12$. Then Theorem 1 implies that $a|c$, i.e., $c/a = 6/3 = 2$ is an integer.
2. *(5 points)* No, let $a = 6$, $b = 2$ and $c = 3$, $\gcd(a, b) = 2$ and $a|bc$ but $a \nmid c$.
3. *(5 points)* Using Bézout's theorem, there exists integers s and t such that $\gcd(a, b) = 1 = sa + bt$. If $a|bc$, then there exists an integer k such that $bc = ka$. Replacing b by ka/c in the first equation we obtain

$$sa + \frac{tka}{c} = 1,$$
$$sac + tka = c,$$
$$a(sc + tk) = c.$$

Since, s, c, k and t are all integers, then $q = sc + kt$ is an integer such that $aq = c$. Therefore, $a|c$.

Problem II: *(10 points)* Consider the following finite sequence

$$a_1 = 7, a_2 = 77, a_3 = 777, a_4 = 7777, \ldots, a_{2003} = \underbrace{77\cdots7}_{\text{2003 times}}.$$

We want to show that there is an element in this sequence that is divisible by 2003. If one of the a_i's is already divisible by 2003, then we are done. Next, we assume that none of the a_i's is divisible by 2003 and show that there is a contradiction.

1. *(5 points)* Assuming that none of the a_i's is divisible by 2003, prove that there exists two elements a_i and a_j, $j > i$, such that $a_j - a_i$ is divisible by 2003.
2. *(5 points)* Note that $a_j - a_i$ is not an element of the sequence. Use Theorem 1 (given below) and the result of the first question to prove that if $a_j - a_i$ is divisible by 2003, then there exists an element a_k in the sequence that is divisible by 2003.

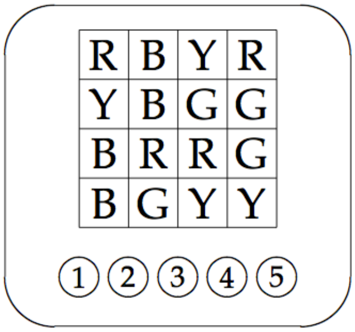
Theorem 1 *If a, b, and c are positive integers such that* $\gcd(a, b) = 1$ *and $a|bc$, then $a|c$.*

Solution:

1. *(5 points)* If no element a_i, $i = 1, \ldots 2003$, of the sequence is divisible by 2003, then all elements a_i can be written as $a_i = q_i 2003 + r_i$ where q_i is an integer and $1 \leq r_i \leq 2002$ is the remainder of the division of a_i by 2003. Since there are 2003 remainders and 2002 possible values for r_i, then by the pigeonhole principle at least two of the remainders r_i and r_j must be equal. Therefore, we can write
$$a_j - a_i = (q_j - q_i)2003 + r_j - r_i = (q_j - q_i)2003.$$
Hence, $a_j - a_i$ is divisible by 2003.

2. *(5 points)* We need to find an element a_k of the sequence that is divisible by 2003. Notice that $a_j - a_i$ can be represented by $j - i$ digits equal to "7" followed by i digits equal to "0" which means that $a_j - a_i$ can be written as $a_j - a_i = a_{j-i}10^i$. We illustrate this idea in the following equation
$$\begin{array}{rl} a_j = & \underbrace{777777\ldots77777}_{j-i}\underbrace{777777}_{i} \\ - & \\ a_i = & \underbrace{777777}_{i} \\ \hline a_j - a_i = & \underbrace{777777\ldots77777}_{a_{j-i}}\underbrace{000000}_{\times 10^i} \end{array}$$
We have that $a_{j-1}10^i$ is divisible by 2003, i.e., 2003 divides $a_{j-1}10^i$. Since 10^i and 2003 are relatively prime, $\gcd(10^i, 2003) = 1$, we can use the result of theorem 1 and deduce that 2003 divides a_{j-i}. In other words, a_{j-1} is divisible by 2003.

Problem III: *(15 points)* An electronic toy displays a 4×4 grid of colored squares. At all times, four are red, four are green, four are blue, and four are yellow. For example, here is one possible configuration:



R	B	Y	R
Y	B	G	G
B	R	R	G
B	G	Y	Y

1. *(5 points)* How many such configurations are possible?

2. *(5 points)* Below the display, there are five buttons numbered 1, 2, 3, 4, and 5. The player may press a sequence of buttons; however, the same button can not be pressed twice in a row. How many different sequences of n button-presses are possible?

3. *(5 points)* Each button press scrambles the colored squares in a complicated, but non-random way. Prove that there exist two *different* sequences of 32 button presses that both produce the *same* configuration, if the puzzle is initially in the state shown above. (Hint: $4^{32} = 16^{16} > 16!$).

Solution:

1. *(6 points)* Method 1:To form a configuration, one needs to accomplish the following tasks:

   a) Choose the location of the 4 red squares, which is equivalent to choosing a subset of 4 elements out of a subset of 16 elements (order does not matter): $\binom{16}{4}$ ways.

   b) And choose the location of the 4 green squares out of the remaining 12 available locations: $\binom{12}{4}$ ways.

   c) And choose the location of the 4 blue squares: $\binom{8}{4}$ ways.

   d) And choose the location of the 4 yellow squares out of the remaining 12 available locations: $\binom{4}{4}$ ways.

   By the product rule, there are $\binom{16}{4} \cdot \binom{12}{4} \cdot \binom{8}{4} \cdot \binom{4}{4} = \frac{16!}{4!4!4!4!}$.

   Method 2: If the squares of the same color were all distinguishable, then there would be 16! configurations (because there are 16! permutations). But, in any of these permutations, we can permute the red squares (4! ways) without changing the configuration in the electronic display, and we can permute the green squares (4! ways), the blue squares (4! ways) and the yellow squares (4! ways) without changing the configuration. By the division rule, the total number of configurations is therefore, $\frac{16!}{4!4!4!4!}$.

2. *(5 points)* To choose a sequence of n button presses, one need to do the following:

   1: Choose which button to press first: 5 possibilities

2: And choose which button to press second: 4 possibilities (cannot press the previous button)

3: And choose which button to press third: 4 possibilities again...

$\vdots$

n-1: And choose which button to press the at the n-1 th time: 4 possibilities

n: And choose which button to press last: 4 possibilities

By the product rule, there are 5.4^{n-1} sequences.

3. *(5 points)* From part b, there are $5.4^{31} > 4^{32} = 16^{16}$ possible button-presses, but $\frac{16!}{4!4!4!4!}$ configurations. Since $16^{16} > 16!$, this means that there are more button presses then configurations. By, the pigeonhole principle, there must be at least two button presses that give the same configuration.

   Note: $n! \leq n^n$. You can prove it by induction.

A	B	C	D	E	F	G	H	I	J	K	L	M
00	01	02	03	04	05	06	07	08	09	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Table 1: The number corresponding to each letter of the alphabet.

Problem IV: *(20 points + 5 bonus points)* To encrypt messages using RSA cryptosystem using a particular key (n, e), you first translate a plaintext message M into sequences of integers using the Table 1. Next, you divide this string into equally sized blocks denoted by m_i. Each block m_i consists of $2N$ digits, where $2N$ is the largest even number such that the number $252525 \cdots 25$ with $2N$ digits does not exceed n. Afterwards, each block m_i is encrypted to a cipher block c_i using the formula $c_i = m_i^e \mod n$. In this problem, we want to encrypt the word GO using the RSA cryptosystem $(2537, 13)$. Note that $n = 2537 = 43 \times 59$.

1. *(2 points)* Translate the plaintext message GO into a number that we call m_i.
2. *(5 points)* Find $m_i^3 \mod 43$ and $m_i^3 \mod 59$. Deduce $m_i^{13} \mod 43$ and $m_i^{13} \mod 59$.
3. *(5 points)* Use Bézout's theorem to find the multiplicative inverse of 43 modulo 59 and the inverse of 59 modulo 43.
4. *(8 points)* Encrypt text message GO using this RSA cryptosystem, i.e., find $c_i = m_i^{13} \mod 2537$. (*Hint:* you can use the previous results and the Chinese remainder theorem.)
5. **BONUS:** *(5 points)* Find $m_i^{59} \mod 59$.

Solution:

1. Using Table 1 we convert GO to $m_i = 0614$.
2. We proceed as follows,

$$\begin{aligned} m_i \mod 43 &= 614 \mod 43 = 12, \\ m_i^3 \mod 43 &= 12^3 \mod 43 = 1728 \mod 43 = 8, \\ m_i^{13} \mod 43 &= 8 \times 8 \times 8 \times 8 \times 12 \mod 43 = 49152 \mod 43 = 3. \end{aligned}$$

Similarly,

$$\begin{aligned} m_i \mod 59 &= 614 \mod 59 = 24, \\ m_i^3 \mod 59 &= 24^3 \mod 59 = 13824 \mod 59 = 18, \\ m_i^{13} \mod 59 &= 18 \times 18 \times 18 \times 18 \times 24 \mod 59 = 2519424 \mod 59 = 6. \end{aligned}$$

3. We first express the $\gcd(59, 43)$ as a linear combination of 43 and 59. Using the Euclidean division we can write the following.

$$\begin{aligned} 59 &= 43 + 16, \\ 43 &= 2 \times 16 + 11, \\ 16 &= 11 + 5, \\ 11 &= 2 \times 5 + 1, \end{aligned}$$

Therefore,

$$\begin{aligned}
1 &= \gcd(59, 43), \\
&= 11 - 2 \times 5, \\
&= 11 - 2 \times (16 - 11), \\
&= 3 \times 11 - 2 \times 16, \\
&= 3 \times (43 - 2 \times 16) - 2 \times 16, \\
&= 3 \times 43 - 8 \times 16, \\
&= 3 \times 43 - 8 \times (59 - 43), \\
&= 11 \times 43 - 8 \times 59.
\end{aligned}$$

Since $11 \times 43 = 1 + 8 \times 59 \implies 11 \times 43 \mod 59 = 1$, then 11 is the inverse of 43 modulo 59. Similarly, $11 \times 43 - 8 \times 59 = 1 \implies -8 \times 59 \mod 43 = 1$, then $-8 \equiv 35(\textbf{mod})43$ is the multiplicative inverse of of 59 modulo 43.

4. Computing $614^{13} \mod 2537$ cannot be done using a calculator, therefore we use the computer arithmetic for large integers method. To find $614 \mod 2537$ we find $614^{13} \mod p$ and $614 \mod q$ where p and q are prime numbers smaller than 2537 and that satisfy $2537 = p \times q$. Then, using the Chinese remainder theorem we find $614^{13} \mod 2537$. We know that $2537 = 43 \times 59$. So we find $614^{13} \mod 43$ and $614^{13} \mod 59$.

   We know that $614^{13} \equiv 3(\textbf{mod}\, 43)$ and $614^{13} \equiv 6(\textbf{mod}\, 59)$. Thus we can use the Chinese remainder theorem to find $614^{13}(\textbf{mod}\, 2537)$. Let $a_1 = 3$, $a_2 = 6$, $m_1 = 43$, $m_2 = 59$ and let x denote the number we want to find. We can write

   $$x = a_1 M_1 y_1 + a_2 M_2 y_2 \mod 2537.$$

   Here, $M_1 = 2537/m_1 = 59$, $M_2 = 43$, $y_1 = 35$ is the inverse of M_1 modulo m_1 and $y_2 = 11$ is the inverse of M_2 modulo M_2. Therefore,

   $$\begin{aligned}
   x &= 3 \times 59 \times 35 + 6 \times 43 \times 11 \mod 2537, \\
   x &= 1422.
   \end{aligned}$$

   The encryption of GO using this RSA cryptosystem is 1422.

Problem V: *(25 points)* Consider a coin for which the probability of heads is p. Note: parts 1 and 2 below can be solved independently.

1. In this part, suppose that we repeatedly and independently flip the coin n times and count the number of heads/tails.

   (a) *(3 points)* In how many ways can we obtain k heads out of the n flips, where $1 \leq k \leq n$?

   (b) *(3 points)* What is the probability that the outcomes of the first k flips are heads, and the outcomes of the remaining flips are tails?

   (c) *(4 points)* What is the probability of obtaining k heads out of n flips? What is the value of this probability for $k = 7, n = 10, p = 0.55$?

   (d) *(4 points)* Given that k heads were obtained. What is the probability that these k heads were obtained in k consecutive flips?

2. In this part, suppose that we repeatedly and independently flip the coin until a head comes up.

   (a) *(3 points)* What is the probability that we stop flipping the coin after completing m flips?

   (b) *(4 points)* Suppose that the probability of stopping after $m = 2$ flips is 0.24. Determine the value(s) of p. Is the coin biased?

   (c) *(4 points)* Let $p = 0.1$. Suppose that you have to choose in advance the number of coin flips that you will make. What is the minimum number of flips that you would choose in order to guarantee above 98% chance of obtaining a head (i.e., stopping)?

Solution:

1. (a) The number of way of obtaining exactly k heads is equal to the number of combinations where k out of n flips are heads. Therefore, the number is $C(n,k) = \binom{n}{k}$.

   (b) Since the coin flips are independent the probability is

$$\underbrace{p \times p \times \ldots p}_{k \text{ times}} \times \underbrace{(1-p) \times (1-p) \times \ldots (1-p)}_{n-k \text{ times}} = p^k(1-p)^{n-k}.$$

   (c) The probability of obtaining k heads is: the probability of obtaining k heads in a specific combination, multiplied by the number of possible combinations. From the previous parts we know that the probability of getting k heads in specific combination (such as k heads in the first k flips) is $p^k(1-p)^{n-k}$. The number of possible combinations is $\binom{n}{k}$. Therefore, the probability of obtaining k heads in n flips is

$$\binom{n}{k} p^k (1-p)^{n-k}.$$

   For $n = 10, k = 7, p = 0.55$ the probability is equal to 0.1665.

   (d) Let E be the event where we obtain k heads out of n flips. Let F be the event where we obtain k heads in k consecutive flips. The question asks to compute $p(F|E)$. From the definition of conditional probability we know that

$$p(F|E) = \frac{p(F \cap E)}{p(E)}.$$

From the previous question we know that $p(E) = \binom{n}{k}p^k(1-p)^{n-k}$. Intuitively we can note that $p(F \cap E) = p(F)$, since event E is included in event F. $p(F)$ is determined by multiplying $p^k(1-p)^{n-k}$ by the number of possible ways of obtaining k consecutive heads. Since the k heads have to be consecutive, the first head could occur in flip 1, or flip 2, ..., or flip $n-k+1$. The possibilities of the position of the first head stop at flip $n-k+1$ because if the first head occurs at flip $n-k$ or further, there will not be enough remaining flips to obtain k heads. Therefore, the number of possible ways of obtaining k consecutive heads is $n-k+1$. Therefore,

$$p(F|E) = \frac{p(F \cap E)}{p(E)} = \frac{p(F)}{p(E)} = \frac{(n-k+1)p^k(1-p)^{n-k}}{\binom{n}{k}p^k(1-p)^{n-k}} = \frac{n-k+1}{\binom{n}{k}}.$$

2. (a) If we stop flipping after m flips, it means that the first $m-1$ flips were tails and the last flip was heads. Therefore, the probability is $(1-p)^{m-1}p$.

   (b) Since the probability of stopping after $m = 2$ flips is 0.24, then $(1-p)p = 0.24 \Rightarrow p - p^2 = 0.24$. Hence, we obtain the following second degree equation

   $$p^2 - p + 0.24 = 0.$$

   The equation has two solutions which are given by

   $$p_1 = \frac{1 + \sqrt{1 - 4(0.24)}}{2} \quad p_2 = \frac{1 - \sqrt{1 - 4(0.24)}}{2}.$$

   Hence, $p_1 = 0.6$ and $p_2 = 0.4$.So p can have two values which are 0.6 or 0.4. In both cases, the coin is biased because $p \neq 0.5$.

   (c) Let G be the event where you obtain a head and stop flipping with m flips. Therefore $\bar{G}$ is the event that you do not obtain a head within m coin flips. You have to choose the number of flips m such that $p(G) > 0.98$. We have $p(G) = 1 - p(\bar{G})$, where $p(\bar{G})$ is the probability of obtaining no heads within m flips, i.e., all tails. We have,

   $$p(\bar{G}) = (1-p)^m.$$

   Therefore, we require that

   $$1 - (1-p)^m > 0.98.$$

   Since $p = 0.1$ we get

   $$\begin{aligned} (0.9)^m &< 0.02 \\ m \ln(0.9) &< \ln(0.02) \\ m &> 37.13. \end{aligned}$$

   Therefore, the minimum number of flips needed is 38.

Problem VI:*(15 points)* Multiple choice questions. Circle only one correct answer.

1. *(3 points)* Let A, B and C be sets.

   (a) If $A \cap C = B \cap C$, then $A = B$.

   (b) If $A \cup C = B \cup C$, then $A = B$.

   (c) If $A \cap C = B \cup C$, then $A = B$.

   [✓ (d)] None of the above.

2. *(3 points)* The compound proposition $\neg(r \to \neg q) \vee (p \wedge \neg r)$ is

   (a) False when p, q and r have the same truth value.

   [✓ (b)] False when p and q are both false.

   (c) False when p is false, q is true and r is true.

   (d) None of the above.

3. *(3 points)* The sum $1/4 - 1/8 + 1/16 - 1/32 + 1/64 - \ldots$ is equal to

   [✓ (a)] 1/6

   (b) 1/4

   (c) 1/2

   (d) 1

   (e) None of the above, your answer: ________

4. *(3 points)* The following is a solution to the recurrence relation $a_n = 4a_{n-1} - 3a_{n-2}$

   [✓ (a)] $a_n = 7 \cdot 3^n - \pi$

   (b) $a_n = 2^n$

   (c) $a_n = (n+1)^2$

   (d) $a_n = \sqrt{n}$

   (e) None of the above, your answer: ________

5. *(3 points)* In a classroom of 25 students, what is the probability that at least 3 students were born on the same day of the week?

   (a) $3/25$

   [✓ (b)] 1

   (c) $\binom{7}{1}\binom{25}{3}/25^7$

   (d) None of the above, your answer: ________

6. *(3 points)* Suppose $g : A \to B$ and $f : B \to C$, where $f \circ g$ is one-to-one and g is one-to-one. Then,

   (a) f must be one-to-one

   (b) f must be onto

   (c) f must be a bijection.

   [✓ (d)] None of the above.