Math 240/ CS 240 Spring 2018 April 11, 2018
Mariya Soskova Midterm II Solutions

I. (15 points.) Each question has only one correct answer. Circle the one you think is correct.

1. Let a be a positive integer divisible by 7, 2, and no other prime. Let b be a positive integer divisible by 5 and 2. Which of the following must be false?

   (a) $a \equiv b \pmod 7$.

   (b) $\underline{a \equiv b \pmod 5}$. (We know that a is not divisible by 5 and b is.)

   (c) $a \equiv b \pmod 2$.

2. What is the multiplicative inverse of 5 in $\mathbb{Z}_7$?

   (a) The number 5 does not have a multiplicative inverse in $\mathbb{Z}_7$.

   (b) $\frac{1}{5}$.

   (c) $\underline{3}$. ($15 \equiv 1 \pmod 7$)

3. What is the complexity of the following algorithm, measured by the number of additions?

```
procedure p($n$ : positive integer)
$x := 0$
for $i := 1$ to n
    for $j := i$ to n
        for $k := i$ to j
            $x := x + 1$
return $x$.
```

   (a) $O(n)$.

   (b) $O(n^2)$.

   (c) $\underline{O(n^3)}$.

4. Which of the following statements is not equivalent to the other two:

   (a) If $P(0)$ is true and $(\forall n)(P(n) \rightarrow P(n+2))$ then P holds for all even natural numbers.

(b) If $P(0)$ is true and $(\forall n)P(n)$ implies $(\forall n)P(n+2)$ then P holds for all even natural numbers. (The other two are equivalent to mathematical induction on the natural numbers. This is a false statement.)

(c) Every nonempty set of even nonnegative integers has a least element.

5. If $A = \{1, 2, 3, 4, 5\}$ and $B = \{a, b, c, d, e, f, g\}$ then the number of injective functions $f : A \to B$ such that $f(1) \in \{a, b\}$ and $f(2) \in \{a, b\}$ is:

   (a) $5 \cdot 4 \cdot 3 \cdot 2$. (We have two choices for $f(1)$. Once $f(1)$ is picked, then $f(2)$ is determined. $f(3)$ can be any letter among the remaining $\{c, d, e, f, g\}$. This leaves 4 possibilities for $f(4)$ and 3 for $f(5)$.)

   (b) $2^2 \cdot 7^3$.

   (c) $6 \cdot 5 \cdot 4 \cdot 3$.

II. (15 points.) True or False? Explain why!

1. If $a \equiv b \pmod{m}$ and $c \equiv b \pmod{m}$ then $a + c \equiv b \pmod{m}$ and $a \cdot c \equiv b \pmod{m}$.

   Answer: False. $5 \equiv 2 \pmod{3}$ and $2 \equiv 2 \pmod{3}$, but $5 + 2 \not\equiv 2 \pmod{3}$ and $5 \cdot 2 \not\equiv 2 \pmod{3}$.

2. If $ab \in S$ and whenever the word w is in S then $awc \in S$ then S contains the word $aaaabccc$.

   Answer: True. Since $ab \in S$, by the rule we get that $aabc \in S$. Applying the rule twice more we get that $aaabcc \in S$ and $aaaabccc \in S$.

3. If you have 10 black socks and 10 white socks, and you are picking socks randomly, you will only need to pick three to find a matching pair.

   Answer: True. Imagine you are putting your socks in 2 boxes: one for white socks, one for black socks. By the pigeonhole principle, once you have put away 3 socks at least one of the boxes will contain at least two socks, so you have a matching pair.

4. Assume inductively that all sets of n horses have the same color. Consider a set of $n + 1$ horses $\{h_1, \ldots h_{n+1}\}$. By the inductive hypothesis $\{h_1, \ldots h_n\}$ are all colored the same and

$\{h_2, \ldots h_{n+1}\}$ are colored the same. So the color of h_1 is the same as the color of $h_2, \ldots h_n$ and that color is the same as that of h_{n+1}. Therefore all $n+1$ horses have the same color and so by induction all horses have the same color.

Answer: False. The reason is explained well on piazza: The argument fails when $n = 1$. That is to say $P(1) \not\Rightarrow P(2)$ because if $H = \{h_1, h_2\}$ is a set of 2 horses, then $A = \{h_1\}$ and $B = \{h_2\}$ are both sets of 1 horse, so all the horses in A are the same color as each other and all the horses in B are the same color as each other, but there's no overlap to transfer the color from h_1 to h_2.

5. If A and B are finite sets of natural numbers then $|\mathcal{P}((A \cup B) \times B)| = 2^{(|A|+|B|)\cdot|B|}$.

Answer: False. If $A \cap B \neq \emptyset$ then $|A \cup B| < |A| + |B|$. For example if $A = B = \{1\}$ then $(A \cup B) \times B = \{(1,1)\}$ and hence$|\mathcal{P}((A \cup B) \times B)| = 2^1 = 2$, but $2^{(|A|+|B|)\cdot|B|} = 2^2 = 4$.

III. (20 points.)

1. Find the prime factorization of 456 and 780. What is the prime factorization of their least common multiple?

Answer: The prime factorization of 456 is $2^3 \cdot 3 \cdot 19$. The prime factorization of 780 is $2^2 \cdot 3 \cdot 5 \cdot 13$. The prime factorization of their least common multiple is $2^3 \cdot 3 \cdot 5 \cdot 13 \cdot 19$. *(Note, that it is also easy to see from the prime factorization that the greatest common divisor of* 456 *and* 780 *is* $2^2 \cdot 3 = 12$).

2. Use Euclid's algorithm to find the greatest common divisor of 456 and 780.

Answer:
$780 = 1 \cdot 456 + 324.$
$456 = 1 \cdot 324 + 132.$
$324 = 2 \cdot 132 + 60$
$132 = 2 \cdot 60 + 12$
$60 = 5 \cdot 12 + 0.$
Therefore 12 is the greatest common divisor of 456 and 780.

3. Convert the number 671 base 10 to base 5.

Answer:
$671 \mod 5 = 1 \quad 671 \text{ div } 5 = 134$
$134 \mod 5 = 4 \quad 134 \text{ div } 5 = 26$
$26 \mod 5 = 1 \quad 26 \text{ div } 5 = 5$
$5 \mod 5 = 0 \quad 5 \text{ div } 5 = 1.$
$1 \mod 5 = 1 \quad 1 \text{ div } 5 = 0.$
Hence, 10141 in base 5 is 671 in base 10.
We can check that we are correct: $1 \cdot 5^4 + 0 \cdot 5^5 + 1 \cdot 5^2 + 4 \cdot 5 + 1 \cdot 5^0 = 625 + 0 + 25 + 20 + 1 = 671.$

4. Solve the linear congruence $5x \equiv 7 \pmod{8}$.

Answer:
The inverse of 5 modulo 8 is 5, because $5 \cdot 5 = 25 \equiv 1 \pmod{8}$. (You can use the algorithm going through Bezout coefficients to find the inverse, as well.) Hence $x \equiv 35 \pmod{8} \equiv 3 \pmod{8}$. The solution is therefore $x = 3 + 8k$, where $k \in \mathbb{Z}$.

IV. (20 points.) Consider the the set S defined inductively as follows:

1. $3 \in S$, $4 \in S$
2. If $x \in S$ and $x \bmod 2 = 1$ then $x + 2 \in S$.
3. If $x \in S$ and $x \bmod 4 = 0$ then $x + 4 \in S$.

1. List 4 even and 4 odd elements of S.

   Answer: $4 \in S$. Applying the second rule, we get: $8, 12, 16 \in S$. Similarly, $3 \in S$ and so applying the first rule $5, 7, 9 \in S$.

2. Prove that the set A of all odd numbers $z \geq 3$ is a subset of S.

   Answer: The set A can be defined as $\{2k+1 \mid k \geq 1\}$. We use induction to show that for every $k \geq 1$ the property $P(k) : 2k + 1 \in S$ is true. The basis of the induction is when $k = 1$. Then $2k+1 = 3 \in S$ by (1). Assume inductively that $P(k)$ is true, i.e. $2k+1 \in S$. Since $2k + 1 \bmod 2 = 1$, we can apply rule (2) to get that $2k + 1 + 2 = 2(k + 1) + 1 \in S$. This proves that $P(k+1)$ is true. By the induction principle, we have that for every $k \geq 1$ the property $P(k)$ is true and so $A \subseteq S$.

3. Prove that $B = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod{4} \wedge x \geq 8\} \subseteq S$.

   Answer: The set B can be defined as $\{4k \mid k \geq 2\}$. We use induction to show that for every $k \geq 2$ the property $P(k) : 4k \in S$ is true. The basis of the induction is when $k = 2$. Then $4k = 8 \in S$ because $4 \in S$ by (1), $4 \bmod 4 = 0$ and so by (3) $4 + 4 = 8 \in S$. Assume inductively that $P(k)$ is true, i.e. $4k \in S$. Since $4k \bmod 4 = 0$, we can apply rule (3) to get that $4k + 4 = 4(k + 1) \in S$. This proves that $P(k + 1)$ is true. By the induction principle, we have that for every $k \geq 2$ the property $P(k)$ is true and so $B \subseteq S$.

4. Prove that $S = A \cup B \cup \{4\}$.

Answer: By the previous two parts of the problem we know that $A \subseteq S$ and $B \subseteq S$. By (1) we know that $4 \in S$. It follows that $A \cup B \cup \{4\} \subseteq S$. What remains to be shown is that $S \subseteq A \cup B \cup \{4\}$. We use structural induction to prove that. The basis of the induction is to prove that $3, 4 \in A \cup B \cup \{4\}$. This is obvious for 4, as $4 \in \{4\}$, and true for 3, as $3 \in A$. Next, suppose inductively that $x \in S \cap A \cup B \cup \{4\}$, where $x \mod 2 = 1$. It follows that $x \geq 3$. Then $x + 2$ is an odd number and $x + 2 \geq 3$, so $x + 2 \in A \subseteq A \cup B \cup \{4\}$. If on the other hand $x \in S \cap A \cup B \cup \{4\}$, where $x \mod 4 = 0$ then $x \geq 4$. It follows that $x + 4 \geq 8$ and $x + 4 \mod 4 = 0$, so $x + 4 \in B \subseteq A \cup B \cup \{4\}$.

V. (10 points.) Prove or refute the following statement: "If you pick five numbers from the integers 1 to 8 then two of them must add up to nine".

Answer: There are 4 ways to get 9 as a sum of two different integers from 1 to 8: $1 + 8$, $2 + 7$, $3 + 6$, and $4 + 5$. When picking numbers from 1 to 8, lets put them in the boxes labelled by these 4 options. By the pigeonhole principle, if we pick 5 numbers at least one box will contain both of its possible numbers, hence we will have picked two that add up to 9.

VI. (20 points.) How many length 10 words w are there in the English alphabet such that:

1. The word w is a palindrome, i.e. reads the same backward as forward. (Example of a palindrome is *madam*.)

Answer: If w is a 10 letter palindrome then we have freedom to choose the first 5 letters, then the first determines the last, the second letter determines the 9th, the 3rd determines the 8th, the 4th determines the 7th and the 5th determines the 6th. The English alphabet has 26 letters, the order matters and repetitions are allowed, so we are looking at permutations of length 5 of 26 letters: altogether there are 26^5 possibilities.

2. w contains the subword *progress*.

Answer: The word progress has 8 letters. If it is a subword of a 10 letter word, there are three possibilities for where it starts: it can be a prefix of the word (start at position 1), it can be the middle of the word (start at position 2), and it can be a suffix of the word (start at position 3). In each case we have two more letters that are free for us to determine. Altogether, this gives $3 \cdot 26^2$ possibilities.

3. w has at least 8 consecutive letters that are the same.

Answer: We have 3 possibilities: w has 8 consecutive letters that are the same, 9 consecutive letters that are the same or 10 consecutive letters that are the same. For the last case, all need is to pick which letter - so there are 26 choices. For the middle case, w can start with 9 consecutive letters that are the same and end in a different letter, for which there are $26 \cdot 25$ choices, or it can start with a letter and end in 9 consecutive letters different from the first letter, so again we have $26 \cdot 25$. Finally if the repeated letters are 8 we have 3 cases: if they are at the beginning of the word, there are 26 possibilities for these, then 25 for the 9-th letter and 26 again for the 10-th. Similarly, if they are at the end we have $26 \cdot 25 \cdot 26$ possibilities and finally if they are in the middle we have $26 \cdot 25 \cdot 25$ possibilities becuase both the first and last letter have to be different from the middle. Altogether, we have $26 + 2 \cdot 26 \cdot 25 + 2 \cdot 26^2 \cdot 25 + 26 \cdot 25^2$ possibilities.

4. At most two different letters appear in w.

Answer: We have 2 cases: only 1 letter appears in w and exactly 2 letters appear in w. For the first case we have 26 choices. For the second we have $\binom{26}{2}$ ways in which we can pick the 2 letters, then 2^{10} possibilities for words with those two letters, but from them we need to remove 2 words: the ones which use only 1 letter. Altogether, we have $26 + \binom{26}{2} \cdot (2^{10} - 2)$ possibilities.