MATH 363 Discrete Mathematics
Solutions: Assignment 5

1 Grading Scheme

1. Out of **2pt**: +1pt If true or false is well decided.

   +1pt If a proof or counterexample is given.

2. Out of **2pt**: +1pt If true or false is well decided.

   +1pt If a proof or counterexample is given.

3. Out of **2pt**: Full marks if message is correct.

4. Out of **3pt**: +2pt If the answer is $\min\{b_1, b_2\}$, for some values as below.

   .5pt for each justification of why $a = b_i (\mathbf{mod}\ m)$.

5. Out of **2pt**: +1pt If answer 6 random numbers is given.

   +1pt if there is some justification given.

6. Out of **3pt**: The proof can be broken in 3 parts.

   1pt for each part in the answer that paraphrases the solution below.

7. Out of **1pt** each: Full marks if answer is correct.

8. Out of **3pt**: The proof can be broken in 3 parts.

   1pt for each part in the answer that paraphrases the solution below.

9. Out of **2pt**: 1pt If the answer is correct.

   +1pt If some justification is given.

10. Out of **2pt**: Full marks if answer paraphrases the one below.

    -1pt If they do not state which is the inverse of 2^{-1}.

11. Out of **3pt**: Full marks if answer paraphrases the one below.

    -1pt If they do not state which integers are inverse of which.

12. Out of **2pt**: 1pt If the answer is correct.

    +1pt If the procedure of modular exponentiation is displayed. (Possible shorcuts $2^3 = 1 (\mathbf{mod}\ 7)$ or $5^3 = -1 (\mathbf{mod}\ 7)$.)

13. Out of **2pt**: +1 if answer is correct.

    +1pt is some justification is given (an explicit linear combination, mention to a theorem of class).

14. Out of **4pt**: +1pt If decryption gives the string 1816200817170411 translated to SQUIRREL.

    +1pt If the decryption function is displayed.

    +1pt If it is explained that encrypted string has to be broken into 4 blocks.

    +1pt If there is a verifycation or argument why 2753 is the inverse of 17 modulo 3120.

Extra If the Euclidean algorithm is used to find the value 2753.

15. Out of **2pt**: +1pt If the basis step is stated and correct.

    +1pt If the inductive step is stated and correct.

2 Assignment with solutions

1. (**2pt**)Prove or disprove that if $a|c$ and $b|d$, then $ab|cd$.
   It is true. The two assumptions of divisibility imply that there are integers k, l such that $c = ka$ and $d = lb$. It follows that $cd = (kl) \cdot ab$ or in other words, ab is a factor of cd.

2. (**2pt**) Prove or disprove that $a|bc$ implies that either $a|b$ or $a|c$.
   It is false. A counterexample is: $a = 2 \cdot 3 = 6$, $b = 10 = 2 \cdot 5$ and $c = 9 = 3^2$. This is an instance where $a|bc$ since $bc = 90 = 6 \cdot 15$ but $a = 6$ is neither a factor of 10 nor 9.

3. (**2pt**) Decode the following message encripted with Caesar's cipher: **Darorwv olyh lq Arfklplofr.**
   The message is: **Axolots live in Xochimilco**

4. (**3pt**) Let $a, m \in \mathbf{Z}$ and $m > 0$. Find a formula for the integer with smallest absolute value that is congruent to $a \ (\mathbf{mod}\ m)$.
   Use the division algorithm to express $a = km + b$ with $0 \leq b < m$. Let s denote the integer with smallest absolute value that is congruent to $a \ (\mathbf{mod}\ m)$.
   Then $|s| = \min\{b, m - b\}$, $s = b - m\lfloor 2b/m \rfloor$; or equivalently $s = \min\{x - \lfloor x/m \rfloor m, \lceil x/m \rceil m - x\}$.
   Justification of these formulas:

   - From the division algorithm and definitions of modular arithmetic we have that b and $b - m$ are two integers congruent to a modulo m. And thus, the absolute value of s is the minimum of $|b| = b$ and $|b - m| = m - b$
   - If $2b < m$, then $s = b$ and $\lfloor 2b/m \rfloor = 0$. If $2b > m$, then $m - b < b$ and so $s = b - m$; note that in this case $\lfloor 2b/m \rfloor = 1$. Finally, if $2b = m$ then m is even and $m - b = b$. With this, we conclude that in any of the three cases, the formula $s = b - m\lfloor 2b/m \rfloor$ gives the right answer.
   - If $b = 0$, then $\lfloor x/m \rfloor = k = \lceil x/m \rceil$ and $s = 0$. If $b \neq 0$, then $\lfloor x/m \rfloor = k$ and $\lceil x/m \rceil = k + 1$. It follows that $b = x - \lfloor x/m \rfloor m$ and $b - m = \lceil x/m \rceil m - x$; which are the two possible values of s.

5. (**2pt**) Consider the linear congruence generated by $x_{n+1} = 2x_n (\mathbf{mod}\ 18)$ with seed $x_0 = 17$. How many pseudorandom numbers can we generate before numbers start repeating?
   Applying the recurrence function we find:
   $x_1 = 2 \cdot 17 \, (\mathbf{mod}\ 18) = 16$,
   $x_2 = 2 \cdot 16 \, (\mathbf{mod}\ 18) = 14$,
   $x_3 = 2 \cdot 14 \, (\mathbf{mod}\ 18) = 10$,
   $x_4 = 2 \cdot 10 \, (\mathbf{mod}\ 18) = 2$,
   $x_5 = 2 \cdot 2 \, (\mathbf{mod}\ 18) = 4$,
   $x_6 = 2 \cdot 4 \, (\mathbf{mod}\ 18) = 8$,
   $x_7 = 2 \cdot 8 \, (\mathbf{mod}\ 18) = 16$.
   Thus, we can generate 6 random numbers before they start repeating themselves.

6. (**3pt**) Prove that there are infinitely many prime numbers.
This proof can be divided in three parts.
First part. Let S be the set that contains all prime numbers. The proof is by contradiction: Assume that S is finite. Then the prime numbers can be listed $S = \{p_1, p_2, \ldots, p_k\}$.
Second part. Let $m = 1 + p_1 \cdot p_2 \cdots p_k$. **Claim.** There is a number $q \notin S$ which divides m and q is prime. If the claim is true, it leads to a contradiction because all prime numbers are assumed to be contained in S.
Third part. Proof of claim above.
Case 1: m is prime (then $m = q$). Consider $p_i \in S$, we have that $m \geq p_1 \cdots p_k \geq p_i$; this implies that $m \neq p_i$. Since this holds for all $p_i \in S$ we conclude that $q \neq S$.
Case 2: m is not prime. Then there is a prime number q that divides m. Again consider $p_i \in S$, suppose that $q = p_i$ since q divides m and q divides $P = p_1 p_2 \cdots p_k$ then q divides $m - P = 1$. This is a contradiction, there is no prime number that divides 1. Thus we conlude that $q \neq p_i$. Since this holds for all $p_i \in S$ we have that $q \neq S$. Completing the proof of the claim in the second part.

7. (**1pt each**) Find the following values and express them as product of prime numbers

   i) $gcd(18, 99)$ $gcd(2 \cdot 3^2, 3^2 \cdot 11) = 3^2$

   ii) $lcm(18, 99)$ $lcm(2 \cdot 3^2, 3^2 \cdot 11) = 2 \cdot 3^2 \cdot 11$

   iii) $gcd(2^3 \cdot 3 \cdot 5^2, 2 \cdot 7 \cdot 5^4) = 2 \cdot 5^2$

   iv) $lcm(2^3 \cdot 3 \cdot 5^2, 2 \cdot 7 \cdot 5^4) = 2^3 \cdot 3 \cdot 5^4 \cdot 7$

8. (**3pt**) Prove or disprove that for any positive integers a, b,

$$a \cdot b = gcd(a, b) \cdot lcm(a, b)$$

This proof has three main steps: First, let $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ and $a = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$.
Second. With this notation, the greatest common divisor are least common multiple of a and b can be written as
$gcd(a, b) = p_1^{\min\{\alpha_1,\beta_1\}} p_2^{\min\{\alpha_2,\beta_2\}} \cdots p_k^{\min\{\alpha_k,\beta_k\}}$,
$lcm(a, b) = p_1^{\max\{\alpha_1,\beta_1\}} p_2^{\max\{\alpha_2,\beta_2\}} \cdots p_k^{\max\{\alpha_k,\beta_k\}}$.
Third. The result follows by noting that, for any real numbers x, y we have that $xy = \min\{x, y\} \max\{x, y\}$. This is proven by cases (If $x = y$ the minimum equals the maximum. Otherwise, if (w.l.o.g.) $\min\{x, y\} = x$ then $\max\{x, y\} = y$).

9. (**2pt each**) Find the inverse of the following numbers

   i) $2(\textbf{mod } 17)$ $2^{-1} = 9(\textbf{mod } 17)$, since $2 \cdot 9 = 18 = 1(\textbf{mod } 17)$

   ii) $3(\textbf{mod } 18)$ $3^{-1}(\textbf{mod } 18)$, does not exist since $gcd(3, 18) > 1$.

10. (**2pt**) Solve the congruence $2x - 5 = 3(\textbf{mod } 17)$
From the above exercise we have that $2^{-1} = 9(\textbf{mod } 17)$, thus The congruence is equivalent to

$$2^{-1}(2x) = (3 + 5)9(\textbf{mod } 17),$$

simplifying we get $x = 4\,(\textbf{mod } 17)$.

11. (**3pt**) Show that $10! = -1(\textbf{mod } 11)$ without explicitly computing $10!$. (Hint: Pair the factors of $10!$ using the inverse of $a(\textbf{mod } 11)$ for $1 \leq a \leq 10$.)
By inspection, we can verify that the pairs $(2, 6), (3, 4), (5, 9), (7, 8)$ are numbers which are inverse of the other modulo 11. Also, the numbers 1 and 10 are inverse of themselves. Thus

$$10! = 1 \cdot (2 \cdot 6)(3 \cdot 4)(5 \cdot 9)(7 \cdot 8) \cdot 10 = 10 = -1(\textbf{mod } 11).$$

12. (**2pt**) Find $5^{268}(\textbf{mod } 7)$ using modular exponentiation.

$$\begin{aligned}
5^{268} &= (25)^{134}(\textbf{mod } 7)\\
&= (3)^{134}(\textbf{mod } 7)\\
&= (9)^{67}(\textbf{mod } 7)\\
&= 2(2)^{66}(\textbf{mod } 7)\\
&= 2(4)^{33}(\textbf{mod } 7)\\
&= 2\cdot 4(4)^{32}(\textbf{mod } 7)\\
&= 1\cdot 16^{16}(\textbf{mod } 7)\\
&= 2^{16}(\textbf{mod } 7)\\
&= 4^{8}(\textbf{mod } 7)\\
&= 16^{4}(\textbf{mod } 7)\\
&= 2^{4}(\textbf{mod } 7)\\
&= 4^{2}(\textbf{mod } 7)\\
&= 16(\textbf{mod } 7)\\
&= 2(\textbf{mod } 7).
\end{aligned}$$

We can also note that $2^3 = 1\,(\textbf{mod } 7)$. In which case we have:

$$\begin{aligned}
5^{268} &= (25)^{134}(\textbf{mod } 7)\\
&= (3)^{134}(\textbf{mod } 7)\\
&= (9)^{67}(\textbf{mod } 7)\\
&= 2(2)^{66}(\textbf{mod } 7)\\
&= 2(8)^{22}(\textbf{mod } 7)\\
&= 2(1)^{22}(\textbf{mod } 7)\\
&= 2(\textbf{mod } 7).
\end{aligned}$$

We can also note that $5^3 = (-2)^3 = -1\,(\textbf{mod } 7)$. In which case we have:

$$\begin{aligned}
5^{268} &= 5(5)^{3\cdot 89}(\textbf{mod } 7)\\
&= 5(-1)^{89}(\textbf{mod } 7)\\
&= -5 = 2(\textbf{mod } 7).
\end{aligned}$$

13. (**2pt each**) What is the smallest positive integer that can be written as a linear combination of (justify your answer)

    i) 5 and 7
    1 is the smallest: $gcd(5,7) = 1 = 3\cdot 5 - 2\cdot 7$

    ii) 4 and 22
    2 is the smallest: $gcd(4,22) = 2 = -5\cdot 4 + 1\cdot 22$
    In this case, 2 is the smallest integer because every linear combination of even numbers is even, so we cannot express 1 as an linear combination of 4 and 22.

14. (**4pt**) What is the original message encrypted using the RSA system with $n = 53\cdot 61$ and $e = 17$ if the encrypted message is 3185203824602550? (To decrypt, first verify that the decryption exponent is $d = 2753 = (17)^{-1}(\bmod 52\cdot 60)$.)
This exercise is comprised of 4 steps

First, $n = 53 \cdot 61 = 3233$ the largest block of letters we can encode is 2 represented with 4 digits. Therefore, the message was encrypted in 4 blocks: 3185, 2038, 2460, 2550
Second, given the key $(3233, 17)$ we need to find the inverse of 17 modulo $3120 = 52 \cdot 60$, since the number 2753 is proposed, we just need to verify it is, in fact the inverse: $1 = 2753 \cdot 17 + (-15)3120$, so that $2753 \cdot 17 = 1(\bmod 3120)$.
Third, with the information above we now have the decoding key $(3233, 2753)$ and the four blocks of ciphertext we will apply the decryption function $D(x) = x^{2753}(\bmod 3233)$.
Fourth, we compute the following:
$D(3185) = 3185^{2753} = 1816(\bmod 3233)$
$D(2038) = 2038^{2753} = 2008(\bmod 3233)$
$D(2460) = 2460^{2753} = 1717(\bmod 3233)$
$D(2550) = 2550^{2753} = 0411(\bmod 3233)$
Translating the blocks of ciphertext back to letters gives: SQUIRREL.

Extra The Euclidean algorithm consist of a sequence of 'division algorithms'; we start with 3120 and 17:
$3120 = 17 \cdot 183 + \mathbf{9}$
$17 = 9 \cdot 1 + \mathbf{8}$
$9 = 8 \cdot 1 + \mathbf{1}$
Now rewrite the equations, leave the remainders (marked in bold) on the left-hand side of the equation:
$\mathbf{9} = 3120 - 17 \cdot 183$
$\mathbf{8} = 17 - 9 \cdot 1$
$\mathbf{1} = 9 - 8 \cdot 1$
Now we will replace terms in the last equation: we sequentially substitute the remainder of the previous equation. You have to keep track of terms in red, do not multiply these factors.

$$\begin{aligned}
\mathbf{1} &= 9 - 8 \cdot 1 \\
&= 9 - (\mathbf{17} - \mathbf{9} \cdot \mathbf{1}) \cdot 1 \\
&= 9 \cdot 2 - 17 \cdot 1 \\
&= (\mathbf{3120} - \mathbf{17} \cdot \mathbf{183}) \cdot 2 - 17 \cdot 1 \\
&= 3120 \cdot 2 - 17 \cdot 367 \\
&= 3120 \cdot (2 - 17) + 17 \cdot (3120 - 367) \\
&= 17 \cdot 2753 - 3120 \cdot 15.
\end{aligned}$$

The third to last equation is already a linear combination of 3120 and 17. But the coefficient of 17 is negative; so we add and substract the term $3120 \cdot 17$ in each of the summands. We get that the inverse of 17 modulo 3120 is $17^{-1} = -367 = 2753(\bmod 3120)$

15. **(2pt)** Let $A = \begin{pmatrix} a_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & a_k \end{pmatrix}$ be an $k \times k$ diagonal matrix. Show that for any $n \in \mathbf{N}$,

$$A^n = \begin{pmatrix} a_1^n & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & a_k^n \end{pmatrix}$$

We will prove this using induction:

The base step:It is true that $A^1 = \begin{pmatrix} a_1^1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & a_k^1 \end{pmatrix}$; because $a_i = a_i^1$ for any real number.

The inductive step: The inductive hypothesis is that for some integer n we have $A^n = \begin{pmatrix} a_1^n & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & a_k^n \end{pmatrix}$

and we will use this fact to compute

$$\begin{aligned}
A^{n+1} = A^n A &= \begin{pmatrix} a_1^n & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & a_k^n \end{pmatrix} \begin{pmatrix} a_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & a_k \end{pmatrix} \\
&= \begin{pmatrix} a_1^{n+1} & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & a_k^{n+1} \end{pmatrix}.
\end{aligned}$$

The last equality follows from the matrix multiplication properties. Note that we get the desired expression of A^{n+1}, completing the inductive step and therefore, completing the proof by induction.