Homework 4
Due: Wednesday, March 9, 2016

All homeworks are due at 12:55 PM in the CS22 bin on the CIT second floor, next to the Fishbowl.

Include our cover sheet or equivalent, write your Banner ID (but not your name or your CS login) on each page of your homework, label all work with the problem number, and staple the entire handin before submitting.

Be sure to fully explain your reasoning and show all work for full credit. Consult the style guide for more information.

Problem 1

a. Find the values of $x$ that satisfy each congruence. If there are infinitely many, list four of them and state the pattern.

i. $x \equiv 5 \pmod{6}$
ii. $x \equiv -8 \pmod{6}$
iii. $x \equiv 12 \pmod{1}$
iv. $x^2 \equiv 1 \pmod{8}$
v. $6 \equiv 12 \pmod{x}$

b. Compute the greatest common divisor of the numbers specified using the Euclidean algorithm. Furthermore, for each pair, express the gcd as a linear combination of the given numbers. Show all steps.

i. 16, 23
ii. 20, 72

c. Use the Euclidean algorithm to find $x$. Show all steps.

i. $3x \equiv 1 \pmod{11}$
ii. $7x \equiv 3 \pmod{19}$
i. \( \{ \ldots, -1, 5, 11, 17, \ldots, 6k + 5, \ldots \} \) (Infinitely many).

ii. \( \{ \ldots, -2, 4, 10, 16, \ldots, 6k + 4, \ldots \} \) (Infinitely many.)

iii. \( \{ \ldots, -2, -1, 0, 1, \ldots, k, \ldots \} \) All integers (Infinitely many)

iv. \( \{ \ldots, -1, 1, 3, 5, \ldots, 2k + 1, \ldots \} \) (Infinitely many)

v. Holds for factors of 6, so \( \{1, 2, 3, 6\} \) (Finitely many)

b. i. 16, 23 Should work down Euclidean Alg and work back up.

\[
\begin{align*}
23 &= 1 \times 16 + 7 \\
16 &= 2 \times 7 + 2 \\
7 &= 3 \times 2 + 1
\end{align*}
\]

Hence, we can see the gcd = 1.

We can now use the above equations to express the gcd as the linear combination of 16 and 23.

This can be done using a modified version of the Euclidean Alg, where we substitute in our results from previous steps. This way, we can obtain the gcd in terms of the first two numbers.

\[
\begin{align*}
23 - 16 &= 7 \\
16 - 2(23 - 16) &= 2 \\
(23 - 16) - 3(3 \times 16 - 2 \times 23) &= 1
\end{align*}
\]

As a result, we have: \( 7 \times 23 - 10 \times 16 = 1 \).

ii. 20, 72 Should work down Euclidean Alg and work back up.

\[
\begin{align*}
72 &= 3 \times 20 + 12 \\
20 &= 12 + 8 \\
12 &= 8 + 4
\end{align*}
\]

Hence, we can see the gcd = 4.

We can now use the above equations to express the gcd as the linear combination of 20 and 72.

This can be done using a modified version of the Euclidean Alg, where we substitute in our results from previous steps. This way, we can obtain the
gcd in terms of the first two numbers.

\[ 72 - 3 \cdot 20 = 12 \]
\[ 20 - (72 - 3 \cdot 20) = 8 \]
\[ (72 - 3 \cdot 20) - (4 \cdot 20 - 72) = 4 \]

As a result, we have: \( 2 \cdot 72 - 7 \cdot 20 = 4 \).

c. Use the Euclidean algorithm to find \( x \). Show all steps.

i. Use Euclidean Alg to find gcd of 3, 11.

\[
11 = 3 \cdot 3 + 2 \\
3 = 2 + 1 \\
2 = 2 \cdot 2 + 0
\]

Hence, we can see the gcd is 1.
Then use this to express the gcd as a linear combination of 3 and 11:

\[
11 - 3 \cdot 3 = 2 \\
3 - (11 - 3 \cdot 3) = 1
\]

So the linear combination is \( 4 \cdot 3 - 1 \cdot 11 = 1 \)
Hence, we can see that \( 3 \cdot 4 \equiv 1 \pmod{11} \).
This shows us that \( x = 4 + 11k \).

ii. Use Euclidean Alg to find gcd of 7, 19.

\[
19 = 2 \cdot 7 + 5 \\
7 = 5 + 2 \\
5 = 2 \cdot 2 + 1 \\
2 = 2 \cdot 1 + 0
\]

Hence, we can see the gcd is 1.
Then use this to express the gcd as a linear combination of 7 and 19:

\[
19 - 2 \cdot 7 = 5 \\
7 - (19 - 2 \cdot 7) = 2
\]
\[(19 - 2 \times 7) - 2(3 \times 7 - 19) = 1\]

So the linear combination is \(3 \times 19 - 8 \times 7 = 1\).
Hence, we can see that \(-8 \times 7 \equiv 1 \pmod{19}\).
This can then be scaled up to (by multiplying through by 3):
\[9 \times 19 - 24 \times 7 = 3.\]
This in turn shows us that \(-24 \times 7 \equiv 3 \pmod{19}\)
This shows us that \(x = -24 + 19k\).

### Problem 2

In how many ways can \(3^{2016} + 2\) be written as the sum of two primes? Justify.

**Solution**

We know that \(3^{2016}\) is odd because the product of odd numbers is odd. Therefore, \(3^{2016}\) can be written in the form \(2k + 1\) where \(k \in \mathbb{N}\). We can rewrite \(3^{2016} + 2\) as \((2k + 1) + 2 = 2(k + 1) + 1\), which is also an odd number. Recall that the sum of two integers is odd only if one of those two integers is odd and the other is even. However, the only even prime is 2, and \(3^{2016}\) isn’t prime at all. Thus, there are zero ways of representing \(3^{2016} + 2\) as the sum of two primes.

### Problem 3

a. Compute the remainder when \(2^{1111} + 4^{3333} + 6^{4444} + 8^{2222}\) is divided by 11.

b. Prove by induction that \(2^{2^n} + 3^{2^n} + 5^{2^n} \equiv 0 \pmod{19}\) for all integers \(n \geq 1\).

**Note:** \(2^{2^n} \neq 4^n\). Remember your order of operations.

**Hint:** Use two base cases. Why might this be helpful?

**Solution**

a. 2, 4, 6, and 8 are all relatively prime with 11. Using Fermat’s Little Theorem, we know that
\[
2^{10} \equiv 1 \pmod{11},
4^{10} \pmod{11} \equiv 1 \pmod{11}
\]
\[ 6^{10} \equiv 1 \pmod{11} \]
\[ 8^{10} \equiv 1 \pmod{11} \]

Let us consider each component of the sum

\[ 2^{1111} + 4^{3333} + 6^{4444} + 8^{2222} \]

individually:

\[ 2^{1111} = 2 \cdot 2^{1110} \]
\[ = 2 \cdot (2^{10})^{111} \]
\[ \equiv 2 \cdot (1)^{111} \pmod{11} \]
\[ \equiv 2 \pmod{11} \]

\[ 4^{3333} = 4^3 \cdot 4^{3330} \]
\[ = 4^3 \cdot (4^{10})^{333} \]
\[ \equiv 4^3 \cdot (1)^{333} \pmod{11} \]
\[ \equiv 9 \pmod{11} \]

\[ 6^{4444} = 6^4 \cdot 6^{4440} \]
\[ = 6^4 \cdot (6^{10})^{444} \]
\[ \equiv 6^4 \cdot (1)^{444} \pmod{11} \]
\[ \equiv 9 \pmod{11} \]

\[ 8^{2222} = 8^2 \cdot 8^{2220} \]
\[ = 8^2 \cdot (8^{10})^{222} \]
\[ \equiv 8^2 \cdot (1)^{222} \pmod{11} \]
\[ \equiv 9 \pmod{11} \]
In summation:

\[ 2^{1111} + 3^{2222} + 4^{3333} + 5^{4444} \equiv (2 + 9 + 9 + 9) \pmod{11} \]
\[ \equiv 29 \pmod{11} \]
\[ \equiv 7 \pmod{11} \]

Thus, the remainder of \( 2^{1111} + 3^{2222} + 4^{3333} + 5^{4444} \) when divided by 11 is 7.

b. Proof. We want to show that \((\forall n \in \mathbb{Z}^+)\) \(2^{2n} + 3^{2n} + 5^{2n} \equiv 0 \pmod{19}\).

Let \( P(n) \) be that \((\mathbb{Z}^+)\) \(2^{2n} + 3^{2n} + 5^{2n} \equiv 0 \pmod{19}\) holds.

**Base Cases:**

\((k = 1)\)

\[ 2^1 + 3^1 + 5^1 \equiv 4 + 9 + 25 \pmod{19} \]
\[ \equiv 38 \pmod{19} \]
\[ \equiv 0 \pmod{19} \]

\((k = 2)\)

\[ 2^2 + 3^2 + 5^2 \equiv 16 + 81 + 625 \pmod{19} \]
\[ \equiv 722 \pmod{19} \]
\[ \equiv 0 \pmod{19} \]

**Inductive Hypothesis:** We will be assuming that \( P(k) \) holds. In other words, we are assuming that \(2^{2k} + 3^{2k} + 5^{2k} \equiv 0 \pmod{19}\).

**Inductive Step:** We want to show that:

\[ 2^{2k+2} + 3^{2k+2} + 5^{2k+2} \equiv 0 \pmod{19} \]

\[ 2^{2k+2} + 3^{2k+2} + 5^{2k+2} = 2^{2k} \cdot 2^2 + 3^{2k} \cdot 2^2 + 5^{2k} \cdot 2^2 \]
\[ = (2^4)^k + (3^4)^k + (5^4)^k \]

Thus, \( 2^{2k+2} + 3^{2k+2} + 5^{2k+2} \equiv 16^{2k} + 81^{2k} + 625^{2k} \pmod{19} \).
\[ \equiv (-3)^{2k} + (5)^{2k} + (-2)^{2k} \pmod{19} \]
We know that because $2^k$ is necessarily even for $k > 0$, we can rewrite $(-3)^{2^k}$ and $(-2)^{2^k}$ as $3^{2^k}$ and $2^{2^k}$, respectively.

Therefore, $(-3)^{2^k} + (5)^{2^k} + (-2)^{2^k} \equiv 3^{2^k} + 5^{2^k} + 2^{2^k} \pmod{19}$

$\equiv 0 \pmod{19}$

By the inductive hypothesis, we’ve shown that the validity of the $k$-th case implies the validity of the $(k + 2)$-th case. Because we’ve provided two base cases, we’ve shown by strong induction that

$(\forall n \in \mathbb{Z}^+) \ 2^{2n} + 3^{2n} + 4^{2n} \equiv 0 \pmod{19}$

\[ \Box \]

**Problem 4**

It’s The Office Olympics, and Oscar and Angela are playing *very, very fun* game. They start with two distinct, positive integers $a$ and $b$ written on a blackboard. On each player’s turn, he or she writes a new positive integer on the board that is the difference of two integers already present on the board. If a player cannot do so, he or she loses.

For example: suppose that 12 and 15 are on the board initially. Angela plays first and writes 3, which is 15 - 12. Then Oscar writes 9 = 12 - 3. Then Angela plays 6 = 15 - 9. Oscar cannot write any new integers, so he loses.

a. Show that every number on the board at the end of the game is a multiple of $\gcd(a, b)$.

b. Show that every positive multiple of $\gcd(a, b)$ up to $\max(a, b)$ is on the board at the end of the game.

c. Describe a strategy that lets Angela win the game every time.

**Solution**

Let $m = \gcd(a, b)$.

a. Proof by contradiction. Assume that, by the end of the game, there are numbers on the board that are not multiples of $m$. Now, consider $z$, the first number generated in the game that was not a multiple of $m$. Note that $z \neq a$
and \( z \neq b \) because, by the definition of the gcd, \( m \mid a \) and \( m \mid b \).

Consider the turn that generated \( z: x - y = z \). Because \( z \) is the first number that is not a multiple of \( m \), we can write \( x = rm \) and \( y = sm \), because \( x \) and \( y \) are both divisible by \( m \). Thus,

\[
\begin{align*}
z &= x - y \\
z &= mr - ms \\
z &= m(r - s)
\end{align*}
\]

Here, we have a contradiction, because earlier, we said that \( z \) is not a multiple of \( m \). Thus, our initial assumption must be false, and by the end of the game, every number must be a multiple of \( m \).

b. Let \( \gcd(a, b) = m \).

First, we will prove that, before the game is over, \( m \) must be on the board. To do this, we’ll show that we can do the Euclidean Algorithm by playing our game. Because the Euclidean Algorithm with \( a \) and \( b \) generates \( m \), this will show that \( m \) can appear on the board. Consider one arbitrary step of the Euclidean Algorithm:

\[
x = ky + r
\]

Note that we can represent this step of the Euclidean Algorithm with \( k \) turns in our game, where \( x \) and \( y \) are two numbers already on the board. Those turns are as follows:

\[
\begin{align*}
x - y &= z_1 \\
z_1 - y &= z_2 \\
\vdots \\
z_{k-1} - y &= r
\end{align*}
\]

where \( z_1, z_2, \ldots, z_k, \) and \( r \) are the new numbers on the board. Thus, each step in the Euclidean Algorithm can be represented as a series of turns in our game. Because \( a \) and \( b \) start on the board, and we can do the Euclidean Algorithm with \( a \) and \( b \), we know that \( m \) can be on the board by the end of the game.

Now let’s say that the \( m \) is not on the board. Then, the game is not over because there are still moves left (namely, those required to do the Euclidean Algorithm). Therefore, we’ve shown that \( m \) must appear on the board.

Now, we will show that, given that \( m \) appears on the board, every positive multiple of \( m \) up to \( \max(a, b) \) is on the board by the end of the game. Let \( c \)
be some positive multiple of \( m \) less than or equal to \( \max(a, b) \). We will show that \( c \) is on the board upon completion of the game. Consider the turn in which \( m \) is generated. We have two cases:

**Case 1:** \( c \) is on the board. In this case, we are done, because, trivially, \( c \) is on the board.

**Case 2:** \( c \) is not on the board. In this case, consider the lowest positive multiple of \( m \) greater than \( c \) that is on the board (the highest value this can be is \( \max(a, b) \)). Call this number \( d \). Now, note that, because \( d > c \) and \( d \) and \( c \) are both multiples of \( m \), we can repeatedly subtract \( m \) from \( d \) until we reach \( c \). Thus, we know we can generate \( c \). If there is a point in the game that \( c \) is not on the board and \( m \) is, the game can’t be over because there are still turns left (namely, subtracting \( m \) from \( d \)). Therefore, we know that \( c \) must be on the board by the end of the game. Because we have shown that an arbitrary positive multiple of \( m \) less than or equal to \( \max(a, b) \), \( c \), must be generated in the game, we have shown that all positive multiples of \( m \) up to \( \max(a, b) \) are on the board by the end of the game.

c. Once again, let \( m = \gcd(a, b) \). In part (a), we proved that every number on the board by the end of the game is a multiple of \( m \). In part (b), we proved that every positive multiple of \( m \) up to \( \max(a, b) \) is generated before the game is over. Together, these imply that the number of numbers on the board at the end of the game is the number of multiples of \( m \) up to \( \max(a, b) \). In other words, the number of numbers on the board at the end of the game is always \( \frac{\max(a, b)}{m} \). Knowing this, if Angela is to employ a winning strategy, she will have Oscar go first if \( \frac{\max(a, b)}{m} \) is even, and have herself go first otherwise.

**Problem 5**

For \( m \in \mathbb{Z} \), define the relation \( R_m \) on \( M = \{1, \ldots, m - 1\} \) by

\[
\{(x, y) \mid \exists a, b \in \mathbb{Z}^+, \text{ such that } x^a \equiv y^b \pmod{m}\}.
\]

a. Prove that \( \forall m \in \mathbb{Z}^+, R_m \) is an equivalence relation.

b. Prove using Fermat’s Little Theorem that, if \( m \) is prime, \( R_m = M \times M \).

**Solution**

a. In order to show that \( R_m \) is an equivalence relation, we must show reflexivity, symmetry, and transitivity.
**Reflexivity** - Let $x \in M$ and $a = b = 1$. Then, we can say that $x^1 \equiv x^1 \pmod{m}$. Thus, $\forall x \in M, (x, x) \in R_m$.

**Symmetry** - Let $(x, y) \in R_m$, then we know that $\exists a, b \in \mathbb{Z}^+ \text{ s.t. } x^a \equiv y^b \pmod{m}$. This implies that $y^b \equiv x^a \pmod{m}$, which satisfies the conditions of the relation. Therefore, $R_m$ is symmetric.

**Transitivity** - Let $(x, y), (y, z) \in R_m$, then we can say that $\exists a, b, c, d \in \mathbb{Z}^+ \text{ s.t. } x^a \equiv y^b \pmod{m}$ and $y^c \equiv z^d \pmod{m}$.

If we raise both terms in the first congruence to the power $c$ and both terms in the second congruence to the power $b$, then we get $x^{ac} \equiv y^{bc} \pmod{m}$ AND $y^{bc} \equiv z^{bd} \pmod{m}$. Thus, $x^{ac} \equiv z^{bd} \pmod{m}$.

We’ve shown reflexivity, symmetry, and transitivity for $R_m$, and we’ve done so using properties of modular arithmetic that hold for all $m \in \mathbb{Z}^+$, so we can conclude that $R_m$ is an equivalence relation.

b. If $m$ is prime, then we know that $\forall x \in M, x^{m-1} \equiv 1 \pmod{m}$. This means that $\forall (x, y) \in M \times M, x^a \equiv y^b \pmod{m}$, where $a = b = m - 1$. Thus, $\forall (x, y) \in M \times M, (x, y) \in R_m$. Since we know that $R_m \subseteq M \times M$ by definition of relations and that $M \times M \subseteq R_m$ by the above, we can conclude that $R_m = M \times M$. 