Math 255 - Spring 2018
Homework 7 Solutions

1. (a) This is true, so we will prove it.

   Since $a \equiv b \pmod{m}$, we have that by definition m divides $a-b$, or there is an integer k with $a-b=km$.

   We now consider a^2-b^2. If we can show that m divides this, then we will know that $a^2 \equiv b^2 \pmod{m}$.

   We have that $a^2-b^2=(a-b)(a+b)$, and substituting our expression above for $a-b$, we have that

   $$a^2-b^2 = km(a+b) = m\left(k(a+b)\right).$$

   Since $k(a+b)$ is an integer, m divides a^2-b^2 and $a^2 \equiv b^2 \pmod{m}$.

   Note: Alternatively we can use Lemma 1, part e) with $c=a$ and $d=b$, and be done. But it is kind of nice to see it directly with the definition.

   (b) This is false, so we disprove it. (We expect this to be false since it is not true that if a, b, c and m are integers with $m>0$, $ac \equiv bc \pmod{m}$ does not imply that $a \equiv b \pmod{m}$, so certainly something is going on.)

   Let $a=2$, $b=4$ and $m=12$. Then $a^2=2^2=4$ and $b^2=4^2=16$, and indeed $4 \equiv 16 \pmod{12}$. However, $2 \not\equiv 4 \pmod{12}$ and $2 \not\equiv -4 \pmod{12}$ (note that $-4 \equiv 8 \pmod{12}$). This is a counter-example so the claim is disproved.

2. If $1848 \equiv 1914 \pmod{m}$, then m divides $1848-1914$. Therefore m must be any one of the divisors of $1848-1914=-66$ that are strictly greater than 1. Those are

   $$2, 3, 6, 11, 22, 33, \text{ and } 66.$$

3. Let n and $n+1$ be any two consecutive integers, so that n^3 and $(n+1)^3$ are consecutive cubes. Their difference is

   $$(n+1)^3-n^3 = 3n^2+3n+1.$$

   We consider the values that this can take modulo 5, by considering the values that n can take modulo 5. We note that by Section 4, Exercise 5, 5 divides $(n+1)^3-n^3$ if and only if $(n+1)^3-n^3 \equiv 0 \pmod{5}$. For our computations we will use Lemma 1 parts d) and e).

   If $n \equiv 0 \pmod{5}$, then $3n^2+3n+1 \equiv 3\cdot 0^2+3\cdot 0+1 \equiv 1 \pmod{5}$. Therefore 5 does not divide the difference in this case.

   If $n \equiv 1 \pmod{5}$, then $3n^2+3n+1 \equiv 3\cdot 1^2+3\cdot 1+1 \equiv 3+3+1 \equiv 7 \equiv 2 \pmod{5}$. Therefore 5 does not divide the difference in this case.

If $n \equiv 2 \pmod 5$, then $3n^2+3n+1 \equiv 3\cdot 2^2+3\cdot 2+1 \equiv 12+6+1 \equiv 19 \equiv 4 \pmod 5$. Therefore 5 does not divide the difference in this case.

If $n \equiv 3 \pmod 5$, then $3n^2+3n+1 \equiv 3\cdot 3^2+3\cdot 3+1 \equiv 27+9+1 \equiv 37 \equiv 2 \pmod 5$. Therefore 5 does not divide the difference in this case.

If $n \equiv 4 \pmod 5$, then $3n^2+3n+1 \equiv 3\cdot 4^2+3\cdot 4+1 \equiv 48+12+1 \equiv 61 \equiv 1 \pmod 5$. Therefore 5 does not divide the difference in this case.

By Section 4, Theorem 2, n must be congruent to $0, 1, 2, 3$ or 4 modulo 5. We have established that in each case 5 does not divide $(n+1)^3 - n^3$, and therefore 5 never divides the difference of two consecutive cubes.

4. We consider whether it is possible to have $n = a^3 + b^3$ for a and b integers, if $n \equiv 4 \pmod 9$.

   To do so, we consider the values that a^3 (and therefore also b^3, since a and b are arbitrary integers) can take modulo 9. To do that, we consider all of the values that a can take modulo 9, and compute its cube. We tabulate this into a table:

a	a^3	$a^3 \pmod 9$	a	a^3	$a^3 \pmod 9$
0	0	0	5	125	8
1	1	1	6	216	0
2	8	8	7	343	1
3	27	0	8	512	8
4	64	1			

   Therefore we see that no matter what a is, the only possibilities for $a^3 \pmod 9$ are $0, 1$ or 8. As we remarked above, this is therefore also the case for b. Up to reordering, the possibilities for the pairs $(a^3 \pmod 9, b^3 \pmod 9)$ are

$$(0,0), (0,1), (0,8), (1,1), (1,8), (8,8).$$

   (We do not care about reordering since reordering will not change the value of the sum $a^3 + b^3 \pmod 9$, and all we care about is showing that it cannot be $4 \pmod 9$.)

   We verify quickly that in each case the sum of the three entries is not $4 \pmod 9$:

$(a^3 \pmod 9, b^3 \pmod 9)$	$a^3 + b^3 \pmod 9$
$(0,0)$	$0 \pmod 9$
$(0,1)$	$1 \pmod 9$
$(0,8)$	$8 \pmod 9$
$(1,1)$	$2 \pmod 9$
$(1,8)$	$9 \equiv 0 \pmod 9$
$(8,8)$	$16 \equiv 7 \pmod 9$

Therefore if $n \equiv 4 \pmod 9$, it cannot be the sum of two cubes, since the sum of two cubes must be $0, 1, 2, 7$ or $8 \pmod 9$.

5. Just for fun, let's use the representatives $-5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6$ for the elements of $\mathbb{Z}/12\mathbb{Z}$. To simplify the notation, we will also simply write r instead of $[r]_{12}$, since we understand that we are working with elements of $\mathbb{Z}/12\mathbb{Z}$, and not integers or elements of a different $\mathbb{Z}/m\mathbb{Z}$.

   (a) We have

$\times$	-5	-4	-3	-2	-1	0	1	2	3	4	5	6
-5	1	-4	3	-2	5	0	-5	2	-3	4	-1	6
-4	-4	4	0	-4	4	0	-4	4	0	-4	4	0
-3	3	0	-3	6	3	0	-3	6	3	0	-3	6
-2	-2	-4	6	4	2	0	-2	-4	6	4	2	0
-1	5	4	3	2	1	0	-1	-2	-3	-4	-5	6
0	0	0	0	0	0	0	0	0	0	0	0	0
1	-5	-4	-3	-2	-1	0	1	2	3	4	5	6
2	2	4	6	-4	-2	0	2	4	6	-4	-2	0
3	-3	0	3	6	-3	0	3	6	-3	0	3	6
4	4	-4	0	4	-4	0	4	-4	0	4	-4	0
5	-1	4	-3	2	-5	0	5	-2	3	-4	1	6
6	6	0	6	0	6	0	6	0	6	0	6	0

   (b) The units are exactly the elements for which 1 appears in the associated row or column. They are the classes represented by

   - -5 (since $(-5) \cdot (-5) \equiv 1 \pmod{12}$),
   - -1 (since $(-1) \cdot (-1) \equiv 1 \pmod{12}$),
   - 1 (since $1 \cdot 1 \equiv 1 \pmod{12}$),
   - and 5 (since $5 \cdot 5 \equiv 1 \pmod{12}$).

   (c) The zero divisors are exactly the elements for which 0 appears at least twice (since $a \cdot 0 \equiv 0 \pmod{12}$, so we need to get 0 some other time to conclude that a is a zero divisor) in the associated row or column. They are the classes represented by

   - -4 (since $(-4) \cdot (-3) \equiv 0 \pmod{12}$),
   - -3 (since $(-3) \cdot (-4) \equiv 0 \pmod{12}$),
   - -2 (since $(-2) \cdot 6 \equiv 0 \pmod{12}$),
   - 0 (since $0 \cdot (-5) \equiv 0 \pmod{12}$),
   - 2 (since $2 \cdot 6 \equiv 0 \pmod{12}$),
   - 3 (since $3 \cdot (-4) \equiv 0 \pmod{12}$),
   - 4 (since $4 \cdot (-3) \equiv 0 \pmod{12}$),
   - and 6 (since $6 \cdot (-4) \equiv 0 \pmod{12}$).

Note that for parts (b) and (c) one could also have used the Theorem from class saying when a represents a unit modulo 12, but it's nice to work it out "by hand."

6. (a) If we do not see a solution right away, we can use our trusty Euclidean algorithm:

$$\begin{aligned} 23 &= 7 \cdot 3 + 2 \\ 7 &= 2 \cdot 3 + 1. \end{aligned}$$

Back-solving, we get

$$\begin{aligned} 1 &= 7 - 3 \cdot 2 \\ &= 7 - 3 \cdot (23 - 3 \cdot 7) \\ &= 7 - 3 \cdot 23 + 9 \cdot 7 \\ &= 10 \cdot 7 - 3 \cdot 23. \end{aligned}$$

Therefore one possible integer solution is $x = 10$ and $y = -3$. (There are of course infinitely many; they are of the form $x = 10 + 23t$ and $y = -3 - 7t$ for t any integer.)

(b) If we reduce the left hand side of $7x + 23y = 1$ to their least residue modulo 23 we get

$$7x + 23y \equiv 7x \pmod{23}.$$

The least residue of the right hand side is 1. Therefore in $\mathbb{Z}/23\mathbb{Z}$, the equation we solved is

$$7x \equiv 1 \pmod{23},$$

which is exactly the equation we are trying to solve now. Therefore a solution is $v = 10$, or in fact, any integer v such that $v \equiv 10 \pmod{23}$.

Alternatively, we may argue that for any integer solution x to part (a), we have

$$7x - 1 = -23y,$$

by rearranging the equation. Since y is an integer, $-23y$ is divisible by 23, and therefore $7x \equiv 1 \pmod{23}$ by definition. Therefore any x that is a solution to part (a) will be a solution to part (b).

7. By assumption and using Theorem 1 from Section 4, we have that there exists an integer ℓ such that

$$x = 1 + \ell m^k.$$

Now if we raise each side to the power of m, we get

$$x^m = (1 + \ell m^k)^m.$$

We expand the right hand side with the binomial formula:

$$\begin{aligned} x^m &= (1+\ell m^k)^m \\ &= \sum_{i=0}^{m} \binom{m}{i} \ell^i m^{ki}. \end{aligned}$$

We note that when $i \geq 2$, then m^{ki} is divisible by m^{k+1}. Therefore much of the sum is zero modulo m^{k+1} and we can write

$$\begin{aligned} x^m &= \sum_{i=0}^{m} \binom{m}{i} \ell^i m^{ki} \\ &\equiv 1 + \binom{m}{1} \ell m^k \pmod{m^{k+1}}. \end{aligned}$$

We now note that $\binom{m}{1} = m$, so that we have nothing other than

$$\begin{aligned} x^m &\equiv 1 + \binom{m}{1} \ell m^k \\ &\equiv 1 + \ell m^{k+1} \pmod{m^{k+1}} \\ &\equiv 1 \pmod{m^{k+1}}. \end{aligned}$$