Homework 7

For practice: 7.2, 7.3, 7.25

To turn in: 7.1, 7.6, 7.10, 7.11, 7.12, 7.15, 7.16, 7.17ab, 7.19

Extra Credit: 7.28

Solutions to graded problems

7-1. Take for example, $a = x = 2$, $b = 0$ and $n = 4$. Then

$$2 \cdot 2 \equiv 0 \cdot 2 \bmod 4 \quad \text{but} \quad 2 \not\equiv 0 \bmod 4.$$

7-6. The last digit in the base 8 expansion of 9^{1000} is just $9^{1000} \bmod 8$. Using the properties of congruences, I compute modulo 8:

$$9^{1000} \equiv 1^{1000} \equiv 1 \bmod 8.$$

That is, the last digit is 1.

Similarly, I compute

$$10^{1000} \equiv 2^{1000} \equiv 2^1 \cdot 2^{999} \equiv 2 \cdot 8^{333} \equiv 2 \cdot 0^{333} \equiv 0 \bmod 8.$$

So the last digit (the last 333 digits, actually) in the base 8 expansion of 10^{1000} is zero.

Finally, I compute

$$11^{1000} \equiv 3^{1000} \equiv 9^{500} \equiv 1^{500} \equiv 1 \bmod 8.$$

So the last digit in the base 8 expansion of 11^{1000} is 1.

7-10. The relation is not an equivalence relation because it fails to be both reflexive and transitive. There are people in the world (e.g. Palestinians in Israeli-occupied territories) who are citizens of no country and therefore not related even to themselves. Moreover, some countries allow dual citizenship (e.g. Switzerland), so it could happen that both Francois and Jean are citizens of France, and Jean and Arnold are citizens of Switzerland, but Arnold and Francois are not citizens of the same country. In other words

$$(\text{Francois, Jean}), (\text{Jean, Arnold}) \in R \text{ but } (\text{Francois, Arnold}) \notin R.$$

7-11.

a) This relation fails to be transitive. For instance $(8,6), (6,9) \in R$, but $(8,9) \notin R$.

b) This relation is an equivalence relation:

- For any $x \in \mathbf{R}$, we have $x = 2^0 x$. So $(x,x) \in R$. That is, the relation is reflexive.
- Suppose that $(x,y) \in R$. Then $x = 2^n y$ for some $n \in \mathbf{Z}$. Thus $y = 2^{-n}x$, so $(y,x) \in R$. That is, the relation is symmetric.
- Suppose that $(x,y),(y,z) \in R$. Then there exist $n,m \in \mathbf{Z}$ such that $x = 2^n y$ and $y = 2^m z$. Consequently, $x = 2^{n+m}z$, and it follows that $(x,z) \in R$. That is, the relation is transitive.

This proves that R is an equivalence relation. □

7.12. To show that R is an equivalence relation, I must show that it is reflexive, symmetric, and transitive.
Reflexive: If $x \in S$, then there exists $j \in \{1,\dots,k\}$ such that $x \in A_j$ because $S = A_1 \cup \ldots \cup A_n$. Therefore, $(x,x) \in R$ (i.e. 'both x and x are in A_j').

Symmetric: If $(x,y) \in R$ then there exists $j \in \{1,\dots,k\}$ such that $x,y \in A_j$. This is the same as saying $y,x \in A_j$. So $(y,x) \in R$.

Transitive: If $(x,y) \in R$ and $(y,z) \in R$ then there exists $i,j \in \{1,\dots,k\}$ such that $x,y \in A_i$ and $y,z \in A_j$. But then $i = j$ because $y \in A_i \cap A_j$, and if i and j were different, the intersection would be empty. So $x,y,z \in A_i$. It follows that $(x,z) \in R$. □

7-15. The flaw is that for a given x there might be *no* $y \in S$ such that $(x,y) \in R$. An example of a relation of this sort is as follows: S is the set of all people and $R \subset S \times S$ is the relation given by $(x,y) \in R$ if and only if x and y both drive trucks and and have the same color eyes. Then R is transitive and symmetric but not reflexive because if x doesn't drive a truck, then x isn't related to anyone (including x).

7-16. For convenience, I number the days of the week 0 through 6 in order beginning with whatever day is Jan 13 (i.e. if Jan 13 is Tuesday, then that's day 0). Observe that with this system, the $n+13$th day of the year will fall on the day of the week numbered $n \bmod 7$. Hence (in a non-leap year)

- January 13th falls on the 0th day of the week, by definition.
- February 13th falls 31 days later than January 13 and thus on the day of the week numbered
$$31 \equiv 3 \bmod 7.$$
- Similarly, March 13th falls on the $3 + 28 \equiv 31 \equiv 3 \bmod 7$ day of the week.
- April 13: $3 + 31 \equiv 6 \bmod 7$.
- May 13: $6 + 30 \equiv 1 \bmod 7$.

- June 13: $1 + 31 \equiv 4 \bmod 7$.
- July 13: $4 + 30 \equiv 6 \bmod 7$.
- August 13: $6 + 31 \equiv 2 \bmod 7$.
- September 13: $2 + 31 \equiv 5 \bmod 7$.
- October 13: $5 + 30 \equiv 0 \bmod 7$.
- November 13: $1 + 31 \equiv 4 \bmod 7$.
- December 13: $4 + 30 \equiv 6 \bmod 7$.

In summary, the 13th falls on the day of the week numbered 0,3,3,6,1,4,6,2,5,0,4,6 as the months go by. In particular, we see that *every* day 0-6 of the week is represented in this sequence and it follows that there's some month in which the 13th falls on Friday. Moreover, no day of the week occurs more than three times in this sequence, so there won't be more than three Friday the 13ths in a non-leap year.

In a leap year, we must add one to all numbers from March 13th on. Thus our sequence of days (modulo 7) becomes 0,3,4,0,2,5,0,3,6,1,5,0. Again all days of the week appear, so there will be a Friday the 13th somewhere among them; and day 0 occurs 4 times, so if January 13 happens to be a Friday in a leap year, there will actually be four Friday the 13ths.

7-17.

a) Initial step: (n=1) $1^3 + 5 \cdot 1 = 6$ which is certainly divisible by 6.

Induction step: Assume that $6|(k^3 + 5k)$—i.e. $k^3 + 5k = 6\ell$ for some $\ell \in \mathbf{Z}$. Then

$$\begin{aligned}
6(k+1)^3 + 5(k+1) &= 6(K^3 + 3k^2 + 3k + 1) + 5k + 5 \\
&= 6k^3 + 18k^2 + 23k + 6 \\
&= (6k^3 + 5k) + 18k^2 + 18k + 6) \\
&= 6\ell + 6(3k^2 + 3k + 1) = 6(\ell + 3k^2 + 3k + 1),
\end{aligned}$$

so 6 divides $6(k+1)^3 + 5(k+1)$, and the induction step is complete.

This proves that $6|(n^3 + 5n)$ for all $n \in \mathbf{N}$. $\square$

b) Any $n \in \mathbf{Z}$ is congruent modulo 6 to 0, 1, 2, 3, 4, or 5. Moreover, 6 divides $n^3 + 5n$ if and only if

$$n^3 + 5n \equiv 0 \bmod 6.$$

Since $n^3 + 5n$ is obtained from n by multiplication and addition, and since these operations are well-defined modulo 6, it is enough to check that the congruence is true for $n \in \{0,1,2,3,4,5\}$. This I can do directly:

$$\begin{aligned}
0^3 + 5 \cdot 0 &\equiv 0 \bmod 6 \\
1^3 + 5 \cdot 1 &\equiv 6 \equiv 0 \bmod 6 \\
2^3 + 5 \cdot 2 &\equiv 18 \equiv 0 \bmod 6 \\
3^3 + 5 \cdot 3 &\equiv 42 \equiv 0 \bmod 6 \\
4^3 + 5 \cdot 4 &\equiv 84 \equiv 14 \cdot 6 \equiv 0 \bmod 6 \\
5^3 + 5 \cdot 5 &\equiv 150 \equiv 25 \cdot 6 \equiv 0 \bmod 6
\end{aligned}$$

So in all cases $n^3 + 5n$ is divisible by 6. □

7-19. I prove the contrapositive of the assertion. Namely, I suppose that none of the integers m, n, p is divisible by 5 (and aim to show that 5 does not divide $m^2+n^2+p^2$). Then modulo 5, each of the numbers m, n, p is congruent to $1, 2, 3$ or 4. It follows (by squaring and reducing mod 5 each of the numbers 1 through 4) that each of the squares m^2, n^2, p^2 is congruent to 1 or 4. Therefore one of the following must occur:

- all three squares are congruent to 1;
- all three are congruent to 4;
- two squares are congruent to 1 and the third to 4;
- two squares are congruent to 4 and the third to 1;

Going down this list, I find that $m^2 + n^2 + p^2$ is congruent to $3, 1, 1,$ or 4 modulo 5. In any case, the expression is never congruent to $0 \bmod 5$, so 5 does not divide $m^2 + n^2 + p^2$ unless at least one of the three numbers m, n, p is divisible by 5. □