Math 283 Spring 2012
Assignment 6 Solutions

Exercise 7.2.

Solution.
An integer written in base 10 is divisible by 5 if and only if the last digit is 0 or 5. It is divisible by 2 if and only if the last digit is even. The last digit does not determine whether it is divisible by 3, since 3 is divisible by 3 but 13 is not. ■

Exercise 7.5.

Solution.
The congruence class of 10^n modulo 11 is $(-1)^n$, and hence $654321 \equiv -3 \mod 11$. The first statement follows from the fact that the congruence class of kl is the congruence class of the product of any representatives of the classes of k and l. Hence we can use 1 instead of 10 in forming the product n times. For the subsequent computation,

$$\begin{aligned} 654321 &\equiv 6(-1)^5 + 5(-1)^4 + 4(-1)^3 + 3(-1)^2 + 2(-1)^1 + (-1)^0 \\ &\equiv -6 + 5 - 4 + 3 - 2 + 1 \equiv -3 \mod 11. \end{aligned}$$

■

Exercise 7.8.

Solution.
Since $9 \equiv 1 \mod 8$, we can rewrite $9^{1000} \equiv 1^{1000} \equiv 1 \mod 8$.
Since $10 = 2 \cdot 5$, 10^1000 is a multiple of $2^3 = 8$, and so the remainder is 0 meaning $10^1000 \equiv 0 \mod 8$.
Since $11 \equiv 3 \mod 8$, we have $11^{1000} \equiv (3^2)^5 00 \equiv 1^{500} \equiv 1 \mod 8$. ■

Exercise 7.10.

Solution.
We factor $k^2 - 1$ as $(k+1)(k-1)$ and observe since k is odd, both of these are even. Let $k - 1 = 2m$ for some $m \in \mathbb{Z}$. This means $k^2 - 1 = 2m(2m+2) = 4(m(m+1))$. Now, either m is even (in which case 8 divides the product) or m is odd, in which case $m+1$ is even and so 8 divides the product. ■

Exercise 7.11.

Solution.
(a) This is not an equivalence relation. It satisfies the reflexive and symmetric properties, but not the transitive property: $(2, 6) \in R$ and $(6, 3) \in R$, but $(2, 3) \notin R$.
(b) This is an equivalence relation:
Reflexive property: $x = 2^0 x$.
Symmetric property: if $x = 2^n y$, then $y = 2^{-n} x$.
Transitive property: if $x = 2^n y$ and $y = 2^m z$, then $x = 2^{n+m} z$. ■

Exercise 7.12.

Solution.
Reflexive property: x and x belong to the same set A_i.
Symmetric property: If x and y belong to A_i, then y and x belong to A_i.
Transitive property: If x and y belong to A_i, and y and z belong to A_j, then $i = j$ since y belongs to only one set (since the sets are disjoint). This means that x and z belong to the same set A_i. ■

Exercise 7.15.

Solution.
The error in the "proof" is when it states "Consider x in S. If $(x, y) \in R$, then the symmetric property implies that $(y, x) \in R$. Now the transitive property applied to (x, y) and (y, x) implies that $(x, x) \in R$."

This argument assumes the existence of an element y different from x such that $(x, y) \in R$, however, there need not be such an element. ■

Exercise 7.17.

Solution.
(a) For $n = 1$, $n^3 + 5n = 6$, which is divisible by 6. Suppose $m^3 + 5m$ is divisible by 6. Then $(m + 1)^3 + 5(m + 1) = (m^3 + 5m) + (3m^2 + 3m) + 6$. Notice that $m^3 + 5m$ is divisible by 6 (inductive hypothesis). Also, $3m^2 + 3m = 3m(m + 1)$ is divisible by 6 since either m or $m + 1$ is even. This means that 6 divides $[(m + 1)^3 + 5(m + 1)]$.
(b) Since $5 \equiv -1 \mod 6$, we have $n^3 + 5n \equiv n^3 - n \equiv (n + 1)n(n - 1) \mod 6$. Since 3 consecutive integers contain at least one even number and a multiple of 3, their product is divisible by 6. Thus $n^3 + 5n$ is also divisible by 6. ■

Exercise 7.18.

Solution.
We factor $2n^2 + n$ as $n(2n + 1)$. Since p is prime, this product is a multiple of p if and only if n is a multiple of p or $2n + 1$ is a multiple of p (i.e. $n = \frac{p-1}{2}$). ■

Exercise 7.20.

Solution.
Since $k \equiv 1 \mod k-1$, we have $k^n - 1 \equiv 1^n - 1 \equiv 0 \mod k-1$. ■

Exercise 7.23.

Solution.
The congruence class of 10^n modulo 11 is $(-1)^n$, since $10 \equiv -1 \mod 11$. If n is a palindrome with $2l$ digits, then $n = \sum_{i=0}^{2l-1} a_i 10^i$ with $a_i = a_{2l-1-i}$. Since $i + 2l - 1 - i$ is odd, the parity of i is opposite to the parity or $2l-1-i$. Therefore, $10^i + 10^{2l-1-i} \equiv 0 \mod 11$. Since $a_i = a_{2l-1-i}$, grouping these pairs gives us that

$$n = \sum_{i=0}^{l-1} a_i(10^i + 10^{2l-1-i}) \equiv \sum_{i=0}^{i-1} a_i \cdot 0 \equiv 0 \mod 11.$$

The proof that every integer whose base k representation is a palindrome of even length is divisible by $k+1$ is the same as the above, just replace "10" with "k" and "11" with "$k+1$". ■

Exercise 7.24.

Solution.
The function $f : \mathbb{Z}_n \to \mathbb{Z}_n$ defined by $f(x) = x^2$ is injective only when $n \leq 2$. If $n > 2$, then -1 and 1 are different classes, but $f(-1) = f(1)$. ■

Exercise 7.28.

Solution.
(a) Each power of 10 is 10 times the previous power, which is congruent to 3 times the previous power when reduced modulo 7. We therefore have $10 \equiv 3 \mod 7$, $10^2 \equiv 2 \mod 7$, $10^3 \equiv -1 \mod 7$, $10^4 \equiv -3 \mod 7$, and $10^5 \equiv -2 \mod 7$.

Using the decimal representation, we obtain

$$535801 \equiv 5(-2) + 3(-3) + 5(-1) + 8(2) + 0(3) + 1(1) = -7 \equiv 0 \mod 7.$$

■

Exercise 7.33.

Solution.

Out of 1500 soldiers, the number x of soldiers that remain satisfies $x \equiv 1 \mod 5, x \equiv 3 \mod 7$, and $x \equiv 3 \mod 11$. Applying the procedure for proving the Chinese Remainder Theorem described in class gives us that:

i	a_i	n_i	N_i	$N_i \mod n_i$	y_i
1	1	5	77	2	3
2	3	7	55	-1	-1
3	3	11	35	2	6

Then we compute

$$(1)(77)(3) + (3)(55)(-1) + (3)(35)(6) = 231 - 165 + 630 = 696.$$

Thus, the set of solutions is the set of integers that are equivalent to $696 \mod 385$, in other words congruent to $311 \mod 385$. Since only a few soldiers deserted, the number remaining should be the largest integer less than 1500 that is congruent to $311 \mod 385$. Since $311 + 3 \cdot 385 = 1466$, we conclude that 34 soldiers deserted. ■

Exercise 7.34.

Solution.

Since 7, 8 and 9 are pairwise relatively prime, we can apply the Chinese Remainder Theorem. We find that

$$x = \sum a_i N_i y_i = 288 - 3 \cdot 64 + 5 \cdot 280 = 1499 \equiv -13 \mod 504.$$

Thus the number -13 is the desired solution. ■

Exercise 7.35.

Solution.

The Chinese Remainder Theorem requires relatively prime moduli, which 6 and 8 are not. However, since $x \equiv 3 \mod 6$ if and only if both $x \equiv 1 \mod 2$ and $x \equiv 0 \mod 3$, replacing $x \equiv 3 \mod 6$ with these two congruences does not change the solutions. Now 2 and 8 are not relatively prime, but $x \equiv 5 \mod 8$ requires x to be odd, so we can remove $x \equiv 1 \mod 2$ as a condition. Thus the solutions to the original problem are equivalent to the solutions for $x \equiv 0 \mod 3, x \equiv 4 \mod 7, x \equiv 5 \mod 8$.

The solutions are congruent to $165 \mod 168$. Interestingly, if instead of $x \equiv 3 \mod 6$, we had $x \equiv 4 \mod 6$, there would be no solutions (since this would require $x \equiv 0 \mod 2$, but $x \equiv 5 \mod 8 \implies x \equiv 1 \mod 2$). ■