Logic and Proof Chapter 19 Exercises

Lyle Kopnicky

December 31, 2018

1. Prove the following properties about divisibility (for any integers a, b, and c):

   - If $a \mid b$ and $a \mid c$ then $a \mid b + c$ and $a \mid b - c$.

     Proof. Since $a \mid b$, there is an integer j such that $aj = b$. Likewise there is an integer k such that $ak = c$. We have $a(j + k) = aj + ak = b + c$, so $a \mid b + c$. We have $a(j - k) = aj - ak = b - c$, so $a \mid b - c$.

   - If $a \mid b$ then $a \mid bc$.

     Proof. Since $a \mid b$, there is an integer k such that $ak = b$. Then $akc = bc$, so $a \mid bc$ with divisor kc.

   - $a \mid 0$.

     Proof. We need an integer k such that $ak = 0$. Choose $k = 0$.

   - If $0 \mid a$ then $a = 0$.

     Proof. If $0 \mid a$, then there is an integer k such that $0k = a$. But $0k = 0$ for any k, so $a = 0$.

   - If $a \neq 0$ then the statements $b \mid c$ and $ab \mid ac$ are equivalent.

     Proof. From $b \mid c$ we have that there is a k such that $bk = c$. But then we have $abk = ac$, so the same k serves as a divisor to show that $ab \mid ac$. In the other direction, if $ab \mid ac$, we have a divisor k such that $abk = ac$. Then, since $a \neq 0$, we can factor it out of both sides of the equation, giving us $bk = c$. Thus $b \mid c$.

   - If $a \mid b$ and $b \neq 0$ then $|a| \leq |b|$.

     Proof. If $a = 0$, then b must be 0 (see above), so $|a| = 0 = |b|$. Otherwise, from $a \mid b$, we have a k such that $ka = b$. Suppose that a and b are positive. Then k must be positive. Since $1 \leq k$, we have $a \leq ka = b$. Now suppose a is positive but b is negative. Then k must be negative. Then $|a| = a \leq -ka = |b|$. Now suppose a is negative but b is positive. Then k must be negative. Then $|a| = -a \leq -ka = b = |b|$. Finally, if a and b are both negative, then k is positive. Then $|a| = -a \leq -ak = -b = |b|$.

2. Prove that for any integer n, n^2 leaves a remainder of 0 or 1 when you divide it by 4. Conclude that $n^2 + 2$ is never divisible by 4.

   Proof. Translating the problem into modular arithmetic, the quotient-remainder theorem says we can have 4 possible remainders when dividing n by 4. By the rule of exponentiation for modular arithmetic, we can compute the remainders for n^2:

   $$\begin{aligned} 0^2 &\equiv 0 \pmod 4 \\ 1^2 &\equiv 1 \pmod 4 \\ 2^2 &\equiv 0 \pmod 4 \\ 3^2 &\equiv 1 \pmod 4 \end{aligned}$$

   Thus the remainder will always be 0 or 1 when dividing n by 4. Therefore, $n^2 + 2$ will be congruent to 2 or 3 modulo 4. So it can never be divisible by 4.

3. Prove that if n is odd, $n^2 - 1$ is divisble by 8.

   Proof. If n is odd, then n will be congruent to 1, 3, 5, or 7 modulo 8. Then we can compute the remainders for $n^2 - 1$:

   $$\begin{aligned} 1^2 - 1 &\equiv 0 &&\equiv 0 \pmod 8 \\ 3^2 - 1 &\equiv 8 &&\equiv 0 \pmod 8 \\ 5^2 - 1 &\equiv 24 &&\equiv 0 \pmod 8 \\ 7^2 - 1 &\equiv 48 &&\equiv 0 \pmod 8 \end{aligned}$$

   Thus, $n^2 - 1$ for odd n will always be divisible by 8.

4. Prove that if m and n are odd, then $m^2 + n^2$ is even but not divisible by 4.

   Proof. If m is odd, then it will be congruent to 1, 3, 5, or 7 modulo 8. Then we can compute the remainders for m^2:

$$\begin{aligned}
1^2 &\equiv 1 &&\equiv 1 \pmod 4\\
3^2 &\equiv 9 &&\equiv 1 \pmod 4\\
5^2 &\equiv 25 &&\equiv 1 \pmod 4\\
7^2 &\equiv 49 &&\equiv 1 \pmod 4
\end{aligned}$$

The same applies to n and n^2. Thus by the rule of addition in modular arithemetic, $m^2 + n^2$ is congruent to $1 + 1 = 2$ modulo 4. Since all multiples of 4 are even, any number congruent to 2 modulo 4 is also even. However, it is not divisible by 4: for that it would have to be congruent to 0 modulo 4.

5. Say that two integers "have the same parity" if they are both even or both odd. Prove that if m and n are any two integers, then $m+n$ and $m-n$ both have the same parity.

   Proof. Any integer is congruent to 0 or 1 modulo 2. The even numbers are congruent to 0, and the odd numbers are congruent to 1. Thus we can use the remainder when dividing by 2 to represent the parity.

   We have four possibilities for the parities of m and n: $(0, 0)$, $(0, 1)$, $(1, 0)$, and $(1, 1)$. By the rule of modular addition, adding m and n will produce a value congruent to the sum of the values to which m and n are congruent. In other words, we can add the parities modulo 2. Likewise, when we subtract n from m, we get a value congruent to the difference of the values to which m and n are congruent:

m	n	$m+n$	$m-n$
0	0	0	0
0	1	1	1
1	0	1	1
1	1	0	0

   As you can see, $m+n$ and $m-n$ are matched in parity.

6. Write 11660 as the product of primes.

   Ans. $11160 = 2^3 \cdot 3^2 \cdot 5 \cdot 31$.

7. List all the divisors of 42 and 198, and find the greatest common divisor by looking at the largest number in both lists. Also compute the greatest common divisor of the numbers by the Euclidean Algorithm.

Ans. The divisors of 42 are: -42, -21, -14, -7, -6, -3, -2, -1, 1, 2, 3, 6, 7, 14, 21, and 42. The divisors of 198 are: -198, -99, -66, -33, -22, -18, -11, -9 , -6, -3, -2, -1, 1, 2, 3, 6, 9, 11, 18, 22, 33, 66, 99, and 198. The common divisors are: -6, -3, -2, -1, 1, 2, 3, and 6. The greatest of those is 6.

By the Euclidean algorithm, we have $\gcd(42, 198) = \gcd(198, 42) = \gcd(42, 30) = \gcd(30, 12) = \gcd(12, 6) = 6$.

8. Compute $\gcd(15, 55)$, $\gcd(12345, 54321)$ and $\gcd(-77, 110)$.

   Ans. By Euclid's algorithm, $\gcd(15, 55) = \gcd(55, 15) = \gcd(15, 10) = \gcd(10, 5) = 5$.

   For the second example: $\gcd(12345, 54321) = \gcd(54321, 12345) = \gcd(12345, 4941) = \gcd(4941, 2463) = \gcd(2463, 15) = \gcd(15, 3) = 3$.

   For the third example: $\gcd(77, 110) = \gcd(110, 77) = \gcd(77, 33) = \gcd(33, 11) = 11$.

9. Show by induction on n that for every pair of integers x and y, $x - y$ divides $x^n - y^n$. (Hint: In the induction step, write $x^{n+1} - y^{n+1}$) as $x^n(x - y) + x^n y - y^{n+1}$.)

   Proof. For the base case, we must show that $x - y$ divides $x^0 - y^0$. But $x^0 - y^0 = 1 - 1 = 0$, and every integer divides 0, so we are done.

   For the inductive step, our hypothesis is that $x-y$ divides x^n-y^n. We must show that $x-y$ divides $x^{n+1}-y^{n+1}$. We can rewrite $x^{n+1}-y^{n+1}$ as $x^n x - x^n y + x^n y - y^n + 1$ and factor out $x-y$ to get $x^n(x-y)+x^n y-y^{n+1}$. Clearly, the first term is divisible by $x-y$, so we can subtract that out. This leaves us with $x^n y - y^{n+1}$, which is just y times $x^n - y^n$, which we know to be divisible by $x - y$ according to our inductive hypothesis.

10. Compute $2^{12} \pmod{13}$. Use this to compute $2^{1212004} \pmod{13}$.

    Ans. Since $2^{12} = 4096$ and $13 \cdot 315 = 4095$, we have $2^{12} \equiv 1 \pmod{13}$. Since $1212004 = 12 \cdot 101000 + 4$, we have $2^{1212004} = (2^{12})^{101000} \cdot 2^4$. The law of exponentiation for modular arithmetic says that if $a \equiv b \pmod{n}$, then $a^k \equiv b^k \pmod{n}$. Since $2^{12} \equiv 1 \pmod{13}$, that tells us that $(2^{12})^{101000} \equiv 1^{101000} = 1 \pmod{13}$. To get to $2^{1212004}$, we have to multiply both sides by 2^4, that is, 16. We are justified in applying this by the law of multiplication in modular arithmetic. The result is that $2^{1212004} = (2^{12})^{101000} \cdot 2^4 \equiv 1 * 2^4 = 16 \equiv 3 \pmod{13}$.

11. Find the last digit of 99^{99}. Can you also find the last two digits of this number?

    Ans. To find the last digit, we need to work in arithmetic modulo 10. Since 99 is 1 less than 100, we have that $99 \equiv -1 \pmod{10}$. We can then raise each side to the 99th power: $99^{99} \equiv (-1)^{99} = -1 \equiv 9 \pmod{10}$. So, the last digit is 9.

    To find the last two digits, we need to work in arithmetic modulo 100. Since 99 is 1 less than 100, we have that $99 \equiv -1 \pmod{100}$. The same logic as above applies, so $99^{99} \equiv (-1)^{99} = -1 \equiv 99 \pmod{100}$. Thus, the last two digits are 99.

    Since odd powers of -1 result in -1, and even powers result in 1, we can see a pattern: the last two digits of an odd power of 99 will be 99, and the last two digits of an even power of 99 will be 01.

12. Prove that $50^{22} - 22^{50}$ is divisible by 7.

    Proof. First, since $7 \cdot 7 = 49$, we have that $50 \equiv 1 \pmod{7}$. Thus $50^{22} \equiv 1^{22} = 1 \pmod{7}$. Since $7 \cdot 3 = 21$, we have that $22 \equiv 1 \pmod{7}$. Thus $22^{50} \equiv 1^{50} = 1 \pmod{7}$. Subtracting the two congruences, we get $50^{22} - 22^{50} \equiv 1 - 1 = 0 \pmod{7}$. Thus $50^{22} - 22^{50}$ is divisible by 7.

13. Check whether the following multiplicative inverses exist, and if so, find them:

    - the multiplicative inverse of 5 modulo 7

      Ans. It must have an inverse, because 5 and 7 are coprime. To help us find the inverse, let's make a table of multiples of 5:

k	$5k$	$5k$ mod 7
1	5	5
2	10	3
3	15	1
4	20	6
5	25	4
6	30	2

      The inverse is the value of k for which $5k \bmod 7 = 1$. So, our inverse is 3.

    - the multiplicative inverse of 17 modulo 21

      Ans. Since $5 \cdot 17 = 85 = 4 \cdot 21 + 1$, the inverse is 5.

- the multiplicative inverse of 4 modulo 14

  Ans. There is no inverse, since 4 and 14 have a common factor of 2.

- the multiplicative inverse of -2 modulo 9

  Ans. Since $4 \cdot (-2) = -8 = (-1) \cdot 9 + 1$, the inverse is 4. This could also be calculated by noting that $-2 \equiv 7 \pmod 9$, then finding the inverse for 7.

14. Find all integers x such that $75x \equiv 45 \pmod 8$.

    Ans. We can cast out 8s from 75 and 45, reducing the problem to finding integers x such that $3x \equiv 5 \pmod 8$. Because 3 and 8 are coprime, there is exactly one integer which will satisfy this congruence. Since $3 \cdot 7 = 21 \equiv 5 \pmod 8$, that number is 7. So the answer is the set of integers which are multiples of 8 plus 7: In other words, the coset $8\mathbb{Z} + 7$.

15. Show that for every integer n the number n^4 is congruent to 0 or 1 modulo 5. Hint: To simplify the computation, use that $4^4 \equiv (-1)^4 \pmod 5$.

    Proof. Here's a table of calculations using the rule of exponentiation for modular arithmetic to show the congruences for each possible congruence of n:

$$\begin{aligned}
0^4 &= 0 & &\equiv 0 \pmod 5\\
1^4 &= 1 & &\equiv 1 \pmod 5\\
2^4 &= 16 & &= 3 \cdot 5 + 1 \equiv 1 \pmod 5\\
3^4 &= 81 & &= 16 \cdot 5 + 1 \equiv 1 \pmod 5\\
4^4 &\equiv (-1)^4 & &\equiv 1 \pmod 5
\end{aligned}$$

16. Prove that the equation $n^4 + m^4 = k^4 + 3$ has no solutions in the integers. (Hint: Use the previous exercise.)

    Proof. If there were some integers n, m, and k such that $n^4 + m^4 = k^4 + 3$, then it would also have to be true that $n^4 + m^4 \equiv k^4 + 3 \pmod 5$. From the previous exercise, we know that any integer raised to the fourth power is congruent to 0 or 1 modulo 5. Therefore $n^4 + m^4$ must be congruent to 0, 1, or 2 modulo 5. And $k^4 + 3$ must be congruent to 3 or 4 modulo 5. Therefore the two sides cannot be congruent to each other. There is therefore no solution to the original equation.

17. Suppose p is a prime number such that $p \nmid k$. Show that if $kn \equiv km \pmod{p}$ then $n \equiv m \pmod{p}$.

    Proof. If $kn \equiv km \pmod{p}$ then there is an integer i such that $kn - km = ip$, that is, $k(n-m) = ip$. Since the left-hand side is divisible by k, the right-hand side must be as well. Since p is prime and does not divide k, k must divide i. So there is an integer j such that $jk = i$.

    We can write $k(n-m) = ip$ as $k(n-m) = jkp$. Note that k cannot be 0, otherwise p would divide it. So we can divide both sides by k to get $n - m = jp$. Therefore $n \equiv m \pmod{p}$.

18. Let n, m and c be given integers. Use Bézout's Lemma to prove that the equation $an + bm = c$ has a solution for integers a and b if and only if $gcd(n,m) \mid c$.

    Proof. Define $d = gcd(n,m)$. Then we must prove the implication in each direction.

    Start with the assumption that $gcd(n,m) \mid c$. Then there is an integer k such that $dk = c$. We know from Bézout's Lemma that there exist integers i and j such that $in + jm = d$. Multiplying on both sides by k, we get $ikn + jkm = dk = c$. Let $a = ik$ and $b = jk$. Then $an + bm = c$.

    In the other direction, assume we have a and b such that $an + bm = c$. Since d divides both n and m, it must divide both an and bm, and $an + bm$, and c.

19. Suppose that $a \mid n$ and $a \mid m$ and let $d = \gcd(n,m)$. Prove that $\gcd(\frac{n}{a}, \frac{m}{a}) = \frac{d}{a}$. Conclude that for any two integers n and m with greatest common divisor d the numbers $\frac{n}{d}$ and $\frac{m}{d}$ are coprime.

    Proof. First of all, it is necessary to assume that n and m are not both zero. If they were, d would be zero, so we could not divide by it.

    To prove that $\gcd(\frac{n}{a}, \frac{m}{a}) = \frac{d}{a}$, we need to prove two things: 1) that $\frac{d}{a}$ divides both $\frac{n}{a}$ and $\frac{m}{a}$, and 2) that any other integer dividing both $\frac{n}{a}$ and $\frac{m}{a}$ must also divide $\frac{d}{a}$.

    Since a divides both n and m, we know that $a \mid d$, by the corollary of Bézout's Lemma. It cannot be zero, otherwise it would not be able to divide both n or m, since at least one of them is nonzero. Thus there exists an integer $\frac{d}{a}$.

    Since $d = \gcd(n,m)$, we know that d divides both n and m. Thus there exist integers $\frac{n}{d}$ and $\frac{m}{d}$.

Then $\frac{d}{a}\frac{n}{d} = \frac{n}{a}$, and $\frac{d}{a}\frac{m}{d} = \frac{m}{a}$, so $\frac{d}{a}$ divides both $\frac{m}{a}$ and $\frac{n}{a}$.

Suppose some integer e divides both $\frac{n}{a}$ and $\frac{m}{a}$. Then there exist integers $\frac{n}{ae}$ and $\frac{m}{ae}$. But if $e > \frac{d}{a}$, then $ae > d$, and we already know that d is the greatest integer dividing both n and m. So $e \leq \frac{d}{a}$.

Thus if n and m have a greatest common divisor d, we have

$$\gcd(\frac{n}{d}, \frac{m}{d}) = \frac{d}{d} = 1,$$

so $\frac{n}{d}$ and $\frac{m}{d}$ are coprime.