Homework 2 Solutions

Tim Smits

1. Prove that for any integer n, that $1 \mid n$ and $-1 \mid n$.

Solution: We have $n = 1 \cdot n$ and $n = (-1) \cdot (-n)$, so that $1 \mid n$ and $-1 \mid n$ as desired.

2. For which integers n is it true that $0 \mid n$?

Solution: We see that $0 \mid n$ if and only if there is some integer k such that $n = 0 \cdot k = 0$. Since $0 = 0 \cdot 0$, this says $0 \mid 0$ so $n = 0$ is the only such integer.

3. For which integers n is it true that $n \mid 0$?

Solution: We see that $0 = 0 \cdot n$ for any n, so that $n \mid 0$ for all n.

4. Why is $\gcd(0, 0)$ not defined?

Solution: Since every integer is a divisor of 0, there is no largest positive divisor, making it impossible to define the gcd.

5. Apply the division algorithm to the following pairs of integers. That is, find (q, r) such that $a = bq + r$ with $0 \leq r < b$.

(a) $(47, 13)$

(b) $(823, 48)$

(c) $(-79, 17)$

(d) $(-6257, 316)$

(e) $(39582723, 8243)$

(f) $(82373852, 29574)$

Solution: We omit the details of the calculation.

(a) $(3, 8)$

(b) $(17, 7)$

(c) $(-5, 6)$

(d) $(-20, 63)$

(e) $(4801, 8080)$

(f) $(2785, 10262)$

6.

(a) Suppose that a, b are integers with $b < 0$. Set $b' = -b$. Apply the division algorithm to a, b' and write the results in terms of b.

(b) Verify that it is still true when b is negative that there exist integers q, r such that $a = bq + r$, but now the bound on r is $0 \leq r < |b|$. This says the division algorithm is true regardless of if b is positive or negative.

(c) Prove the uniqueness of q and r in this more general theorem.

Solution:

(a) By the division algorithm, we may write $a = b'q + r$ with $0 \leq r < b'$. Since $b' = -b$, this says $a = -bq + r$ with $0 \leq r < -b$.

(b) If $b < 0$, with $b' = -b$ part a) says $a = -bq + r = b(-q) + r$ with $0 \leq r < -b$, so that in general we may write $0 \leq r < |b|$ regardless of if b is positive or negative.

(c) Suppose that there are integers q, q' and r, r' with $0 \leq r, r' < |b|$ such that $a = bq + r$ and $a = bq' + r'$. Then $bq + r = bq' + r'$ says $b(q - q') = r' - r$. Since b divides the left hand side, this says $b \mid (r' - r)$. However, $0 \leq r, r' < |b|$, so we must have $0 \leq |r' - r| < |b|$. Since $b \mid (r' - r)$ if and only if $|b| \mid (r' - r)$, the only way this is possible is if $|r' - r| = 0$, i.e. $r' = r$. This then says that $b(q' - q) = 0$, and since $b \neq 0$, we get $q = q'$ as desired.

7. Apply the stronger division algorithm to the following pairs of integers. That is, find (q, r) such that $a = bq + r$ with $0 \leq r < |b|$.

(a) $(47, -13)$

(b) $(956, -27)$

(c) $(29657452, -4382)$

Solution: We omit the details of the calculation.

(a) $(-3, 8)$

(b) $(-35, 11)$

(c) $(-6768, 76)$

8.

(a) Prove that for any natural numbers a, b, that $2^a - 1$ divides $2^{ab} - 1$.

(b) Show that if $2^n - 1$ is prime, for some integer n, then n is prime.

(c) Is the converse of the above true?

Solution:

(a) Notice that $2^{ab} - 1 = (2^a)^b - 1$. Use the factorization $x^b - 1 = (x - 1)(1 + x + \ldots + x^{b-1})$ with $x = 2^a$ to see that $2^{ab} - 1 = (2^a - 1)(1 + \ldots + 2^{ab-b})$, so that $(2^a - 1) \mid (2^{ab} - 1)$.

(b) We prove the contrapositive. If n is not prime, write $n = ab$ for some integers a, b with $1 < a, b < n$. Then $2^n - 1 = 2^{ab} - 1$ which is divisible by $2^a - 1$ by part a. Since $a > 1$, $2^a - 1 > 1$, and since $a < n$ we have $2^a - 1 < 2^n - 1$. This says that $2^a - 1$ is a non-trivial divisor of $2^n - 1$, so it is not prime.

(c) No. For $p = 11$, we have $2^{11} - 1 = 2047 = 23 \cdot 89$.

9. Let P be a proposition about integers, and assume the following statements are true:

(a) $P(0)$ is true.

(b) for all $k \in \mathbb{Z}$, $P(k) \implies P(k+1)$.

(c) for all $k \in \mathbb{Z}$, $P(k) \implies P(k-1)$.

Prove that $P(n)$ is true for all $n \in \mathbb{Z}$.

Solution: Conditions a) and b) along with the principle of mathematical induction immediately show that $P(k)$ is true for $k \geq 0$. Define a proposition Q by $Q(k) = P(-k)$. Notice that $Q(0)$ is true, and since $P(-k) \implies P(-k-1) = P(-(k+1)) = Q(k+1)$, we see that $Q(k) \implies Q(k+1)$. Therefore by induction, we see that $Q(n)$ is true for all $n \geq 0$, i.e. $P(n)$ is true for all $n \leq 0$. Putting this together, $P(n)$ is true for all $n \in \mathbb{Z}$.

10. Is the previous result still true if we change the base case from $k = 0$ to some other $k = k_0 \in \mathbb{Z}$?

Solution: Yes, the choice of base case is irrelevant. Since $P(k_0)$ is true, induction says $P(n)$ is true for all $n \geq k_0$, and the above arguement still works to show that $P(n)$ is true for all $n \leq k_0$, i.e. for all $n \in \mathbb{Z}$.