

Problem Set #7 Solutions

Note: There is more than one way in which certain questions can be proved. What we've provided here for each question is just one of those alternatives. The main purpose of these solutions is to serve as models for future proofs that you write. We have been fairly concise, but giving more detail is always acceptable.

1. If n is an integer and $n^3 + 5$ is odd, then n is even.

Proof. We will show the contrapositive. That is, we will show that:

If n is not even, then $n^3 + 5$ is not odd.

Equivalently: If n is odd, then $n^3 + 5$ is even.

Suppose that n is odd. An odd integer multiplied by an odd integer is also odd, so n^2 is also odd. By the same reasoning, n^3 is odd as well. An odd integer (n^3) added to another odd integer (5) yields an even integer. Therefore $n^3 + 5$ is even. We have thus shown the contrapositive, proving the original theorem. (Note: the fact that the product of two odd numbers is odd is right on the borderline of what can be assumed obvious and what should be proved. Here we have omitted the (short) proof, but including it would also be fine.) ■

2. The product of two irrational numbers is irrational.

False. It was shown in LPL that $\sqrt{2}$ is irrational, but $(\sqrt{2})(\sqrt{2}) = 2$ by the definition of the square root. But 2 is rational, since $2 = 2/1$. Thus we have a counterexample. ■

3. If n is an integer ≥ 2 , then there are no primes between $n! + 2$ and $n! + n$.

($n!$ means n factorial, which is the product of the integers from 1 to n .)

Proof: Each number in the range in question is of the form $n! + k$, where $2 \leq k \leq n$. Expanding the factorial, the form is $1 \cdot 2 \cdot 3 \cdot \dots \cdot n + k$. But k divides the product, since it is one of the numbers in the list, and k divides itself. Thus k divides the sum, and the sum is not prime. This is true for all k in the stated range, so there are no primes in that range. ■

4. If n is an odd integer, then $n^2 \equiv 1 \pmod{8}$.

Proof. Suppose n is an odd integer. Then there exists an integer k such that $n = 2k + 1$, and

$$n^2 = (2k + 1)(2k + 1)$$

$$n^2 = 4k^2 + 4k + 1$$

$$n^2 = 4(k^2 + k) + 1$$

$$n^2 = 4(k(k + 1)) + 1$$

But one of k and $k + 1$ is even, so there is an integer m such that $k(k + 1) = 2m$. So

$$n^2 = 4(2m) + 1$$

$$n^2 = 8m + 1$$

So $8 \mid (n^2 - 1)$, i.e., $n^2 \equiv 1 \pmod{8}$. ■

5. Prove or disprove: If $a, b,$ and m are positive integers, then $a \bmod m + b \bmod m = (a + b) \bmod m.$

This statement is false because $a \bmod m + b \bmod m$ can be greater than $m - 1$.
Suppose that $a = 5, b = 6,$ and $m = 7$. Then

and
$$a \bmod m + b \bmod m = 5 \bmod 7 + 6 \bmod 7 = 5 + 6 = 11$$
$$(a + b) \bmod m = (5 + 6) \bmod 7 = 11 \bmod 7 = 4$$

So
$$a \bmod m + b \bmod m \neq (a + b) \bmod m$$

making this a counterexample. The basic problem is that the value on the right must be in the range 0 to $m - 1$, but the sum on the left can be as large as $2(m - 1)$. ■

6. $\phi(5) = 4, \phi(9) = 6, \phi(11) = 10, \phi(12) = 4$

7. n is prime iff $\phi(n) = n - 1.$

Proof. We need to prove this in both directions (forgetting this is a common mistake).

Recall that $\phi(n)$ is the number of positive integers less than or equal to n that are relatively prime to it.

Suppose $n > 1$ is prime. Then it has no divisors other than itself and 1 , and therefore $1, 2, \dots, n - 1$ are relatively prime to it. n is not relatively prime to itself, so if n is prime, $\phi(n) = n - 1$.

Suppose $\phi(n) = n - 1$. We know that $n > 1$, since $\phi(1) = 1$, a contradiction to the supposition. By the definition of ϕ , there are $n - 1$ positive integers less than or equal to n that are relatively prime to it. Since n is not relatively prime to itself, the numbers $1, 2, \dots, n - 1$ are all relatively prime to n , which means that none of these numbers divides n , so n is prime.

Therefore n is prime iff $\phi(n) = n - 1$. ■

8. If $a, b,$ and c are integers, then $c \mid a$ and $c \mid b$ if and only if $c \mid \gcd(a,b).$

Suppose that $c \mid a$ and $c \mid b$. By Bézout's Identity there are integers u, v such that

$$au + bv = \gcd(a,b)$$

But by the assumption above there are integers r, s such that

$$a = cr \text{ and } b = cs$$

Substituting the second equations into the first we get

$$cru + csv = \gcd(a, b)$$

$$c(ru + sv) = \gcd(a, b)$$

This implies that $c \mid \gcd(a, b)$.

Now suppose that $c \mid \gcd(a, b)$. We also know that $\gcd(a, b) \mid a$, so by the transitivity of divides (Theorem 32.3) we have that $c \mid a$. By a similar argument we can show that $c \mid b$. ■

9. If a and b are integers with greatest common divisor d , then $c = ax + by$ for some integers x and y if and only if c is a multiple of d .

Proof. For both directions of the biconditional proof assume that $d = \gcd(a, b)$.

Suppose that $c = ax + by$. Since $d \mid a$ and $d \mid b$, we know that $d \mid ax$ and $d \mid by$. Thus $d \mid c$, which is equivalent to saying that c is a multiple of d .

Suppose that c is a multiple of d . Then $c = rd$ for some integer r . By Bézout's Identity there are integers u, v such that

$$d = au + bv$$

Multiplying by r , we get

$$rd = aur + bvr$$

and thus

$$c = aur + bvr$$

So $c = ax + by$ where $x = ur$ and $y = vr$. ■

10. If n is a positive integer such that the sum of its divisors is $n + 1$, then n is prime.

Proof. Since 1 and n divide n , the sum of the divisors is at least $n + 1$. If it is $n + 1$, then there are no other divisors, so n is prime. ■

11. If $ax \bmod n = ay \bmod n$ and $\gcd(a, n) = 1$, then $x \bmod n = y \bmod n$. (a, x, n, y are positive integers)

Proof.

$ax \bmod n = ay \bmod n$	given
$n \mid ax - ay$	by Theorem 32.12
$n \mid a(x - y)$	factoring
$\gcd(a, n) = 1$	given
$n \mid (x - y)$	by Theorem 32.9
$x \bmod n = y \bmod n$	by Theorem 32.12 ■

12. If a, b , and m are integers such that $m \geq 2$ and $a \equiv b \pmod{m}$, then $\gcd(a, m) = \gcd(b, m)$.

Proof.

$a \equiv b \pmod{m}$	given
$m \mid (a - b)$	definition of congruence
$mn = (a - b)$	for some integer n by definition of divides
$a = b + nm$	algebra
$\gcd(a, m) = \gcd(b, m)$	by Theorem 32.4 ■

13. Suppose n has the prime-power factorization

$$n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$$

where p_1, p_2, \dots, p_k are distinct primes.

Show that for any integers a and b , if $a \equiv b \pmod{n}$ then

$$a \equiv b \pmod{p_i^{e_i}} \text{ for each } i = 1, \dots, k.$$

Proof. Suppose $a \equiv b \pmod{n}$. Then $n \mid (a - b)$, and there is an integer m such that $nm = a - b$. We can rewrite this as

$$p_1^{e_1} p_2^{e_2} \dots p_k^{e_k} m = (a - b)$$

Each $p_i^{e_i}$ divides the LHS, so each must also divide the RHS. So therefore we have that

$$a \equiv b \pmod{p_i^{e_i}} \text{ for each } i = 1, \dots, k. \quad \blacksquare$$

14. Given a positive integer n , there are n consecutive odd positive integers that are primes.

We will show that the statement is false by considering the case $n = 4$. Suppose $k, k + 2, k + 4,$ and $k + 6$ are consecutive odd numbers. As a special case, if $k = 1$, then the four numbers are not prime because 1 is not prime. Otherwise, let $r = k \pmod{3}$. If $r = 0$, then k and $k + 6$ are divisible by 3, so the four numbers are not all prime. If $r = 1$, then $k + 2$ is divisible by 3, and if $r = 2$, then $k + 4$ is divisible by 3. Thus four consecutive odd numbers cannot all be prime, and $n = 4$ is a counterexample. (Note that the statement is true for $n = 3$ since 3, 5, 7 are all prime.) \blacksquare