SOLUTIONS
Math 345
Homework 4
9/27/2017

Exercise 13. Consider positive integers a, b, and c.

(a) Suppose $\gcd(a, b) = 1$.

(i) Show that if a divides the product bc, then a must divide c.

I give two proofs here, to illustrate the different methods.

Proof 1: Using only ch. 6 results. Since $\gcd(a, b) = 1$, we have

$$ax + by = 1 \qquad \text{for some } x, y \in \mathbb{Z}.$$

Multiplying both sides by c gives

$$acx + bcy = c.$$

Since $a|acx$ (by observation) and $a|bcy$ (because $a|bc$), we must have that $a|c$. ☐

Proof 2: using ch. 7 results. If $a \nmid c$, then there is some prime p and positive integer n with

$$p^n|a \quad \text{and} \quad p^n \nmid c$$

Let m be the largest integer such that $p^m|c$, so that $c = c'p^m$ and $p \nmid c'$. Since $m < n$, we also have

$$a' = a/p^m \in \mathbb{Z}.$$

<u>Claim 1:</u> $a' \nmid c'$.

This is because otherwise, there would be some k such that $a'k = c'$. So $ak = p^m a'k = p^m c' = c$, a contradiction.

<u>Claim 2:</u> $a'|bc'$.

Since $a|bc$, there is some integer ℓ satisfying $a\ell = bc$. Dividing both sides by p^m gives $a'\ell = c'b$, verifying our claim.//

<u>Claim 3:</u> $\gcd(a', b) = 1$

Since $a'|a$, any common divisor to a' and b would have to be a common divisor of a and b. So our claim follows from $\gcd(a, b) = 1$. //

Putting these all together, we have

$$p|a' \quad \text{and} \quad a'|bc', \qquad \text{so} \quad p|bc'.$$

Therefore, either $p|c'$ (which it doesn't) or $p|b$ (implying that a' and b have a non-trivial common factor, which they don't). This is a contradiction, implying that $a|c$ after all. ☐

(ii) Show that if a and b both divide c, then ab must also divide c.

Again, I give multiple proofs here, to illustrate the different methods.

Proof 1: Using only ch. 6 results. Since $\gcd(a, b) = 1$, we have $\operatorname{lcm}(a, b) = ab/1 = ab$. So since c is a common multiple of a and b, we have $ab = \operatorname{lcm}(a, b)|c$. $\square$

Proof 2: Using only ch. 6 results. Since $a|c$ and $b|c$ there are $k, \ell \in \mathbb{Z}$ satisfying $ak = c$ and $b\ell = c$. And since $\gcd(a, b) = 1$, we have an integer solution to $ax + by = 1$. Multiplying both sides by k, we get

$$\begin{aligned} k &= akx + bky \\ &= cx + bky && \text{since } ak = c, \\ &= b\ell x + bky && \text{since } c = b\ell, \\ &= b(\ell x + ky). \end{aligned}$$

So

$$c = ak = ab(\ell x + ky).$$

Therefore, since $\ell x + ky \in \mathbb{Z}$, we have $ab|c$. $\square$

Proof 3: using ch. 7 results. If $ab \nmid c$, then there is some prime p and positive integer n such that p^n that divides ab but not c. Since $\gcd(a, b) = 1$, using the fundamental theorem of arithmetic, we must have p^n divides a or b (otherwise, p would divide both). Without loss of generality, suppose $p^n|a$. But then, since $a|c$, we have $p^n|c$, a contradiction. $\square$

(b) Give examples of a, b, and c where $\gcd(a, b) \neq 1$ and...

(i) a divides the product bc, but a does not divide c:

Answer. Let $a = 6$, $b = 3$, $c = 2$. $\square$

(ii) a and b both divide c, but ab does not divide c:

Answer. Let $a = 6$, $b = 9$, $c = \operatorname{lcm}(a, b) = 6 * 9/3 = 18$. $\square$

Exercise 14. Let s and t be odd integers with $s > t \geq 1$ and $\gcd(s,t) = 1$. Prove that the three numbers

$$st, \qquad \frac{s^2 - t^2}{2}, \qquad \text{and} \qquad \frac{s^2 + t^2}{2} \tag{$*$}$$

are pairwise relatively prime (i.e. each pair of them is relatively prime). This fact was needed to complete the proof of the Pythagorean triples theorem (Theorem 2.1 on page 17). [Hint. Assume that there is a common prime factor and use the fact (Lemma 7.1) that if a prime divides a product, then it divides one of the factors.]

Answer. We showed that a Pythagorean triple (a, b, c) is primitive if and only if $\gcd(a, b) = 1$ (i.e. there is no need to check the pairs a and c or b and c, since any pairwise common divisor will imply the others). So since (**??**) forms a Pythagorean triple, we analyze $\gcd(st, (s^2 - t^2)/2)$.

Suppose for the sake of contradiction that $\gcd(st, (s^2 - t^2)/2) > 1$. Then consider a prime divisor p that they have in common (since $\gcd(st, (s^2 - t^2)/2)$ has a prime factorization, such a p exists). Then since $p|st$, we have $p|s$ or $p|t$.

Now using $p|(s^2 - t^2)/2$ to write $(s^2 - t^2)/2 = pb'$ with $b' \in \mathbb{Z}$, we have

$$2pb' = s^2 - t^2 = (s + t)(s - t).$$

So $p|(s + t)(s - t)$, which implies $p|(s + t)$ or $p|(s - t)$. Either way, since $p|s$, this implies that $p|t$. But that implies that p is a common divisor of s and t, contradicting $\gcd(s, t) = 1$.

A similar argument follows for $p|t$. Thus (**??**) forms a PPT.

□

Exercise 15. Group the numbers $-10 \leq i \leq 10$ into sets according to which numbers are pairwise congruent modulo 4. [You should have 4 sets of roughly the same size.]

Answer. Denoting

$$[r] = \{i \in \{-10, \ldots, 9, 10\} \mid i \equiv_4 r\},$$

we have

$$\begin{aligned}
[0] &= \{-8, -4, 0, 4, 8\}, \\
[1] &= \{-7, -3, 1, 5, 9\}, \\
[2] &= \{-10, -6, -2, 2, 6, 10\}, \\
[3] &= \{-9, -5, 3, 7\}.
\end{aligned}$$

□

Exercise 16. Fix $n \geq 1$.

(a) Prove that congruence is an equivalence relation by showing

(i) reflexivity: $a \equiv a \pmod{n}$ for all $a \in \mathbb{Z}$;

(ii) symmetry: if $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$; and

(iii) transitivity: if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.

Proof. Recall that $a \equiv b \pmod{n}$ if and only if $n|(a-b)$, i.e. there is some $k \in \mathbb{Z}$ satisfying $nk = a - b$.

(i) Reflexivity: $a \in \mathbb{Z}$, we have $a - a = 0 = 0 \cdot n$. So $a \equiv_n a$.

(ii) Symmetry: If $a \equiv b \pmod{n}$, then there is a $k \in \mathbb{Z}$ satisfying $nk = a-b$. So $n(-k) = b-a$. Thus, since $-k \in \mathbb{Z}$, we have $b \equiv a \pmod{n}$.

(iii) Transitivity: If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then there are $k, \ell \in \mathbb{Z}$ satisfying

$$nk = a - b \quad \text{and} \quad n\ell = b - c.$$

Therefore

$$a - c = (a-b) + (b-c) = nk + n\ell = n(k+\ell).$$

So since $k + \ell \in \mathbb{Z}$, we have $a \equiv c \pmod{n}$.

$\square$

(b) Suppose $a_1 \equiv b_1 \pmod{n}$ and $a_2 \equiv b_2 \pmod{n}$.

(i) Show that $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$ and $a_1 - a_2 \equiv b_1 - b_2 \pmod{n}$

(ii) Show that $a_1 a_2 \equiv b_1 b_2 \pmod{n}$.

Proof. Since $a_1 \equiv b_1 \pmod{n}$ and $a_2 \equiv b_2 \pmod{n}$, we have $k_1, k_2 \in \mathbb{Z}$ satisfying

$$nk_1 = a_1 - b_1 \quad \text{and} \quad nk_2 = a_2 - b_2. \qquad (**)$$

(i) Using (**??**), we have

$$\begin{aligned}(a_1 + a_2) - (b_1 + b_2) &= (a_1 - b_1) + (a_2 - b_2) \\ &= nk_1 + nk_2 = n(k_1 + k_2), \quad \text{ and } (a_1 - a_2) - (b_1 - b_2) &= (a_1 - b_1) - (a_2 - b_2) \\ &= nk_1 - nk_2 = n(k_1 - k_2).\end{aligned}$$

So since $k_1 \pm k_2 \in \mathbb{Z}$, we have $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$ and $a_1 - a_2 \equiv b_1 - b_2 \pmod{n}$

(ii) Rearranging (**??**), we have

$$a_1 = nk_1 + b_1 \quad \text{and} \quad a_2 = nk_2 + b_2.$$

So

$$\begin{aligned}a_1 a_2 &= (nk_1 + b_1)(nk_2 + b_2) \\ &= n^2 k_1 k_2 + n(k_1 b_2 + k_2 b_1) + b_1 b_2 \\ &= n(nk_1 k_2 + k_1 b_2 + k_2 b_1) + b_1 b_2,\end{aligned}$$

giving

$$a_1 a_2 - b_1 b_2 = n(nk_1 k_2 + k_1 b_2 + k_2 b_1).$$

Therefore, since $(nk_1 k_2 + k_1 b_2 + k_2 b_1) \in \mathbb{Z}$, we have $a_1 a_2 \equiv b_1 b_2 \pmod{n}$.

$\square$

(c) Division.

(i) Give an example of a, b, c, and n, with $c \not\equiv 0 \pmod{n}$, where

$$ac \equiv bc \pmod{n}, \qquad \text{but} \qquad a \not\equiv b \pmod{n}.$$

Example. Let $a = c = 2$, $b = 7$, and $n = 10$: we have $2 \not\equiv 7 \pmod{10}$, but

$$2 * 2 = 4 \equiv 4 \pmod{10}, \qquad \text{and}$$
$$2 * 7 = 14 \equiv 4 \pmod{10}.$$

$\square$

(ii) Show that if $\gcd(c, n) = 1$, then

$$ac \equiv bc \pmod{n} \qquad \text{implies} \qquad a \equiv b \pmod{n}.$$

Proof. If $ac \equiv bc \pmod{n}$, then $n | ac - bc = (a - b)c$. So, since $\gcd(c, n) = 1$, by Exercise 13(a)(i), we have $n | (a - b)$. Thus $a \equiv b \pmod{n}$.

$\square$