

Solutions to In-Class Problems Week 6, Wed.

Problem 1. This problem lets you practice proving simple facts about divisibility.

(a) Prove: If $a \mid b$ and $a \mid c$, then $a \mid sb + tc$ for all s, t .

Solution. Suppose that $a \mid b$ and $a \mid c$. Then there exist integers k_1 and k_2 such that $ak_1 = b$ and $ak_2 = c$. Thus, $sb + tc = s(ak_1) + t(ak_2) = a(sk_1 + tk_2)$, which implies that $a \mid sb + tc$. ■

(b) A number is *perfect* if it is equal to the sum of its positive divisors, other than itself. For example, 6 is perfect, because $6 = 1 + 2 + 3$. Similarly, 28 is perfect, because $28 = 1 + 2 + 4 + 7 + 14$. Explain why $2^{k-1}(2^k - 1)$ is perfect if $2^k - 1$ is prime.

Solution. If $2^k - 1$ is prime, then the only divisors of $2^{k-1}(2^k - 1)$ are:

$$1, 2, 4, \dots, 2^{k-1}$$

which sum to $2^k - 1$ and

$$1 \cdot (2^k - 1), 2 \cdot (2^k - 1), 4 \cdot (2^k - 1), \dots, 2^{k-2} \cdot (2^k - 1)$$

which sum to $(2^{k-1} - 1) \cdot (2^k - 1)$. Adding these two sums gives $2^{k-1}(2^k - 1)$, so the number is perfect. ■

Problem 2. Suppose that we have water jugs with capacities a and b . Use induction to prove that the amount of water in each jug is always a linear combination of a and b and at least one jug is either empty or full. Recall that the allowable operations are to fill a jug with water, empty a jug onto the sidewalk, or to transfer water from one jug to another until one the first one is empty or the second one is full.

In Die Hard 6, the water jugs have capacities 3 and 6 gallons, and Bruce must form 4 gallons of water. As a corollary to the above, prove that Bruce dies.

Solution. To prove the first part, we use induction. Let $P(n)$ be the proposition that after n steps, the amount of water in each jug is a linear combination of a and b .

Base case. $P(0)$ is true, because both jugs are initially empty, and $0 \cdot a + 0 \cdot b = 0$.

Inductive step. Now we must show that $P(n)$ implies $P(n + 1)$ for $n \geq 0$. So assume that after n steps the amount of water in each jug is a linear combination of a and b . There are two cases:

- If we fill a jug from the fountain or empty a jug into the fountain, then that jug is empty or full. The amount in the other jug remains a linear combination of a and b . So $P(n + 1)$ holds.
- Otherwise, we pour water from one jug to another until one is empty or the other is full. By our assumption, the amount in each jug is a linear combination of a and b before we begin pouring:

$$\begin{aligned}j_1 &= s_1 \cdot a + t_1 \cdot b \\j_2 &= s_2 \cdot a + t_2 \cdot b\end{aligned}$$

After pouring, one jug is either empty (contains 0 gallons) or full (contains a or b gallons). Thus, the other jug contains either $j_1 + j_2$ gallons, $j_1 + j_2 - a$, or $j_1 + j_2 - b$ gallons, all of which are linear combinations of a and b .

The lemma follows by the principle of induction.

We now show that Bruce dies. The amount in each jug is always of the form $3s + 6t$ by the above lemma. This is always a multiple of 3 by Problem 1.a, so he can not measure out 4 gallons. ■

Problem 3. Prove: Every common divisor of a and b divides $\gcd(a, b)$.

Solution. For some s and t , $\gcd(a, b) = sa + tb$. Let c be a common divisor of a and b . Since $c \mid a$ and $c \mid b$, we know that c divides $sa + tb = \gcd(a, b)$ by part (a) of problem 1. ■

Problem 4. There is a pond. Inside the pond there are n pebbles, arranged in a cycle. A frog is sitting on one of the pebbles. Whenever he jumps, he lands exactly k pebbles away in the clockwise direction, where $0 < k < n$. The frog's meal, a delicious worm, lies on the pebble right next to his, in the clockwise direction.

(a) Describe a situation where the frog can't reach the worm.

Solution. If $k \mid n$ (say $k = 3$ and $n = 6$), then no number of jumps will lead the frog to the worm, as the frog will be returning to his original pebble ad infinitum. ■

(b) In a situation where the frog can actually reach the worm, explain how to use the Pulverizer (see the appendix of this handout for a description of the Pulverizer) to find how many jumps the frog will need.

Solution. Suppose the frog can reach the worm. When he actually reaches it, he has jumped a number of times, say j , and he has travelled around the cycle a number of times, call it c . Then, the distance that the frog has covered is both $j \cdot k$ and $c \cdot n + 1$, so that

$$jk = cn + 1.$$

But this means that 1 can be written as a *linear combination* of n and k :

$$(-c)n + jk = 1.$$

Since 1 is positive, we conclude that it is a *positive linear combination* of n and k . And since it is the smallest positive integer, we also conclude that it is the *smallest positive linear combination* of n and k . But we have seen in lecture that the smallest positive linear combination of two integers is their GCD. So, the GCD of n and k is 1:

$$\gcd(n, k) = 1$$

and we can use the Pulverizer to find $-c$ and j . ■

(c) Compute the number of jumps if $n = 50$ and $k = 21$. Anything strange?

Solution. We go through the steps as described in the appendix to get that $1 = 8 \cdot 50 - 19 \cdot 21$, or $1 = -(-8) \cdot 50 + (-19) \cdot 21$. Hence, $c = -8$ and $j = -19$, which makes little sense. What does it mean for the frog to make -19 jumps?

The point is that the Pulverizer is guaranteed to give us the integers coefficients of a linear combination that equals the GCD, but it promises nothing about the signs of those coefficients—which, in this case we wanted them to be $-$ and $+$. To get coefficients of the desired sign, we have to think more.

So, we know $1 = 8 \cdot 50 - 19 \cdot 21$. Or, to obtain meaningful signs for the numbers, $19 \cdot 21 = 8 \cdot 50 - 1$. That is, after 19 jumps the frog will have covered 8 full cycles but 1 pebble. So, he will be right next to his original pebble, but in the counter-clockwise direction. Given this, how can he reach the pebble he is after?

Well, if he makes 19 more jumps, he will land 2 pebbles away from his original position in the counter-clockwise direction. Another 19 jumps will lead him 3 pebbles away, and so on. After a total of 49 sets of 19 jumps, he will be 49 pebbles away from its original position in the counter-clockwise direction, which is of course the worm's pebble. Then, the frog will have made $49 \cdot 19 = 931$ jumps.

Here is the table produced by the Pulverizer:

x	y	$(x \text{ rem } y)$	$= x - q \cdot y$
50	21	8	$= 50 - 2 \cdot 21$
21	8	5	$= 21 - 2 \cdot 8$ $= 21 - 2 \cdot (50 - 2 \cdot 21)$ $= -2 \cdot 50 + 5 \cdot 21$
8	5	3	$= 8 - 1 \cdot 5$ $= (50 - 2 \cdot 21) - 1 \cdot (-2 \cdot 50 + 5 \cdot 21)$ $= 3 \cdot 50 - 7 \cdot 21$
5	3	2	$= 5 - 1 \cdot 3$ $= (-2 \cdot 50 + 5 \cdot 21) - 1 \cdot (3 \cdot 50 - 7 \cdot 21)$ $= -5 \cdot 50 + 12 \cdot 21$
3	2	1	$= 3 - 1 \cdot 2$ $= (3 \cdot 50 - 7 \cdot 21) - 1 \cdot (-5 \cdot 50 + 12 \cdot 21)$ $= \boxed{8 \cdot 50 - 19 \cdot 21}$
2	1	0	

■

A Appendix: The Pulverizer

Euclid's algorithm for finding the GCD of two numbers relies on repeated application of the equation:

$$\gcd(a, b) = \gcd(b, a \text{ rem } b)$$

For example, we can compute the GCD of 259 and 70 as follows:

$$\begin{aligned} \gcd(259, 70) &= \gcd(70, 49) && \text{since } 259 \text{ rem } 70 = 49 \\ &= \gcd(49, 21) && \text{since } 70 \text{ rem } 49 = 21 \\ &= \gcd(21, 7) && \text{since } 49 \text{ rem } 21 = 7 \\ &= \gcd(7, 0) && \text{since } 21 \text{ rem } 7 = 0 \\ &= 7. \end{aligned}$$

The Pulverizer goes through the same steps, but requires some extra bookkeeping along the way: as we compute $\gcd(a, b)$, we keep track of how to write each of the remainders (49, 21, and 7, in the example) as a linear combination of a and b (this is worthwhile, because our objective is to write the last nonzero remainder, which is the GCD, as such a linear combination). For our example, here is this extra bookkeeping:

x	y	$(x \text{ rem } y)$	$= x - q \cdot y$
259	70	49	$= 259 - 3 \cdot 70$
70	49	21	$= 70 - 1 \cdot 49$ $= 70 - 1 \cdot (259 - 3 \cdot 70)$ $= -1 \cdot 259 + 4 \cdot 70$
49	21	7	$= 49 - 2 \cdot 21$ $= (259 - 3 \cdot 70) - 2 \cdot (-1 \cdot 259 + 4 \cdot 70)$ $= \boxed{3 \cdot 259 - 11 \cdot 70}$
21	7	0	

We began by initializing two variables, $x = a$ and $y = b$. In the first two columns above, we carried out Euclid's algorithm. At each step, we computed $x \text{ rem } y$, which can be written in the form $x - q \cdot y$. (Remember that the Division Algorithm says $x = q \cdot y + r$, where r is the remainder. We get $r = x - q \cdot y$ by rearranging terms.) Then we replaced x and y in this equation with equivalent linear combinations of a and b , which we already had computed. After simplifying, we were left with a linear combination of a and b that was equal to the remainder as desired. The final solution is boxed.