M109 HW2 Solutions

1

Prove that $\forall n, 2|n(n+1)$.

Proof. The idea is that one of the numbers n, $n+1$ is definitely even, so their product has to be even.

Rigorously: by definition, we have to show that $n(n+1)$ equals $2k$ for some integer k. We perform a case analysis: n is either even or odd.

In the first case, $n = 2m$ for some m. Then $n(n+1) = 2m(2m+1)$ and we set $k := m(2m+1)$.

In the second case, $n = 2m+1$ for some m. Then $n(n+1) = (2m+1)(2m+2) = 2\cdot(m+1)(2m+1)$, and we set $k := (m+1)(2m+1)$.

[We use that even numbers are of the form $2m$ and odd ones are of the form $2m+1$. This was shown in the lecture.] □

2

Suppose p is prime: $p > 1$ and $p|ab \implies p|a \vee p|b$. Show that $p = ab \implies p = \pm a \vee p = \pm b$.

Proof. We have implications $p = ab \implies p|ab \implies p|a \vee p|b$, where the first follows immediately from the definition of divisibility and the second is (part of) the definition of a prime. So, having established $p|a \vee p|b$, we can do case analysis. Assume $p|a$. Then by definition, $a = kp$ for some k. Then we have $p = ab = (kp)b$, so $p = pkb$, or $p(kb-1) = 0$. It follows that $kb - 1 = 0$, so $k = b = \pm 1$ and from $p = ab$ it then follows that $p = \pm a$. Similarly, the case $p|b$ leads to $p = \pm b$. □

3

Prove that

$$d|a, a|b \implies d|b$$

for integers a, b, d.

Proof. By definition, $\exists k \in \mathbb{Z} : a = kd$; $\exists k' \in \mathbb{Z} : b = k'a$. Together these two give $b = k'a = k'(kd) = (kk')d$, so there exists an integer $m := k \cdot k'$ such that $d = m \cdot d$, which means by definition that $d|b$. □

4

For integers d, n, m, r, s,

$$d|m, d|n \implies d|sn + rm$$

.

Proof. We again use the definition: $\exists k : m = dk$; $\exists k' : m = dk'$.

Then we get $sn + rm = s \cdot (dk) + r \cdot (dk')$. Since we are looking for k'' such that $sn + rm = k'' \cdot d$, we should seek to factor d out from the expression we have for $sn + rm$, which we can readily do: $sn + rm = s \cdot (dk) + r \cdot (dk') = d \cdot (sk + rk')$. Thus we set $k'' := sk + rk'$. □

5

True or false: $6|ab \implies 6|a \vee 6|b$? *This is false:*

Proof. Let $a := 2, b := 3$. Then $6|ab$ but 6 can not divide a or b. Indeed, it can never be the case that a greater positive number divides a smaller positive one: if $d|c$ then $c = kd$ for some $k \geq 1$, so $c = k \cdot d \geq 1 \cdot d = d$.

[Note that by problem 2 we conclude that 6 is not prime.] □

6

Prove that $\forall n > 0$,

if n has a divisor d such that $1 < d < n$, then n has a divisor d' such that $1 < d' \leq \sqrt{n}$.

Proof. Take d whose existence we assume. That it is a divisor by definition means that $n = d \cdot d''$ for some integer d''. Now the idea is that if a product of two numbers is n then one of them is at least $\sqrt{n}$. Thus we claim that the integer d' that we are seeking can be taken to be d or d''. That is, we claim $(1 < d \leq \sqrt{n}) \vee (1 < d'' \leq \sqrt{n})$. First, $1 < d$ by assumption and $1 < d''$ because $d < n$. The rest we prove by contradiction. Assume $\neg(d \leq \sqrt{n} \vee d'' \leq \sqrt{n}) = \neg(d \leq \sqrt{n}) \wedge \neg(d'' \leq \sqrt{n}) = (d > \sqrt{n}) \wedge (d'' > \sqrt{n})$, that is, that both d and d'' are greater than $\sqrt{n}$. But then $n = d \cdot d'' > \sqrt{n} \cdot d'' > \sqrt{n} \cdot \sqrt{n} = n$ by properties of the ordering $>$. We get $n > n$, which is a contradiction.

□

7

Prove that for any positive real x, y,

$$\sqrt{xy} \geq \frac{2}{\frac{1}{x} + \frac{1}{y}}.$$

Proof. We have

$$\frac{2}{\frac{1}{x} + \frac{1}{y}} = \frac{2xy}{x + y,}$$

so we need

$$\sqrt{xy} \geq \frac{2xy}{x + y,}$$

or equivalently

$$1 \geq \frac{2\sqrt{xy}}{x + y}$$

$$x + y \geq 2\sqrt{xy}$$

$$x + y - 2\sqrt{xy} \geq 0$$

$$x - 2\sqrt{x}\sqrt{y} + y \geq 0$$

$$\sqrt{x}^2 - 2\sqrt{x}\sqrt{y} + \sqrt{y}^2 \geq 0$$

$$(\sqrt{x} - \sqrt{y})^2 \geq 0,$$

which is of course true.

[This is the "HM-GM"-part of of the chain known as "HM-GM-AM-QM inequalities". Note that in the process we reduced it to the "GM-AM"-part.]

□