Homework 7 Answers
David Rubinstein - Math 100 - Fall 2019

7-20) There exists an n for which $11|2^n - 1$.

Solution: n=10 works. $2^{10} = 1024$ and 1024-1=1023 is divisible by 11.
Fun fact: this is true for any number less than 11 actually. Once can prove that for any number $a < 11, a^{10} \equiv 1 \mod 11$. In fact, there is nothing special about 11, other than it is a prime. So really one can show that for any prime p, and $a < p$, we have $a^{p-1} \equiv 1 \mod$ p. This is called "Fermat's Little Theorem" (same Fermat as the "Fermat's Last Theorem") and we might prove it later this quarter; but I recommend looking it up if you are curious!
In fact, there is a one line proof of this theorem using group theory, and the fact that Z_p is a group (see supplemental problem from HW 5)!!
(You can actually generalize this result even more to non prime integers, using the so called "euler-phi function" and group theory, definitly ask me about this if you are intested)

7-22) If $n \in \mathbb{Z}$ then $4|n^2$ or $4|n^2 - 1$.

Solution: This is saying that for all integers, $n^2 \equiv 0 \mod 4$ or $n^2 \equiv 1 \mod 4$. This is my question 1b on Section 6 assignments. If you have questions about it email me or come to my office hours!

7-30) Suppose a,b integers and p a prime. Show that if $p|ab$ then $p|a$ or $p|b$.

Solution: Note that for any integer x we have gcd(x,p) $= \begin{cases} 1 \text{ if p} \nmid \text{x} \\ p \text{ if p } |\text{x} \end{cases}$.
Then WLOG assume $p \nmid a$ (since if it did we would have nothing to prove). Then gcd(a,p)=1 so we can find integers q,r such that 1=qa +rp. Now multiply both sides by b to get b=qab + rbp. Finally we have p divides ab, and p divides rp so p must divide b.

(7-34) Prove that if gcd(a,c)=gcd(b,c)=1 then gcd(ab,c)=1

Solution: Assume $gcd(ab, c) \neq 1$. Then there is some integer x that divides ab and c. Take some prime $p|x$, then by transitivity of division, $p|ab$ and $p|c$. Yet since p is prime this means $p|a$ or $p|b$. WLOG assume $p|a$; yet this contradicts that gcd(a,c)=1.
(I am cheating a bit here; I used that every integer has a prime number dividing it; there are certainly proofs of this that don't use that fact, yet this is a slick proof I think)

(8-12) If A, B, C are sets then $A - (B \cap C) = (A - B) \cup (A - C)$

Solution: Note if $x \notin B \cap C$ then x is either not in B or not in C. Hence $A - (B \cap C) = \{x : x \in A, x \notin B \cap C\} = \{x : x \in A, x \notin B \text{ or } x \notin C\} = \{x : x \in A - B \text{ or } x \in A - C\} = (A - B) \cup (A - C)$

(8-20) Prove that $A = \{9^n : n \in \mathbb{Q}\} = \{3^n : n \in \mathbb{Q}\} = B$

Solution: Let $x \in A$. Then $x = 9^{\frac{a}{b}} = 3^{\frac{2a}{b}} \in B$. Hence $A \subseteq B$. Now let $y \in B$. Then $y = 3^{\frac{a}{b}} = 9^{\frac{a}{2b}} \in A$. Hence $B \subseteq A$ so A=B.

(8-22) Prove $A \subseteq B$ iff $A \cap B = A$.

Solution: Suppose $A \subseteq B$. Note $A \cap B \subseteq A$ always so we just need to show $A \subseteq A \cap B$. To that end, let a $\in A \subseteq B$. Thus $x \in B$ so $x \in A \cap B$, showing that $A = A \cap B$.
Now suppose $A \cap B = A$, we want to show that $A \subseteq B$. To that end let a $\in A = A \cap B$. Hence in particular a $\in B$, so $A \subseteq B$.

(8-28) Prove that $A = \{12a + 25b : a, b \in \mathbb{Z}\} = \mathbb{Z}$.

Solution: Clearly $A \subseteq \mathbb{Z}$, so we just want to show $\mathbb{Z} \subseteq A$. Let $z \in \mathbb{Z}$. Then we can write z as z=12(-2z)+ 25(z) where $-2z, z \in \mathbb{Z}$. Hence z $\in A$ so $\mathbb{Z} \subseteq \mathbb{Z}$.