REVIEW PROBLEMS FOR SECOND 3200 MIDTERM

PETE L. CLARK

1)a) State Euclid's Lemma (the one involving prime numbers and divisibility).
b) Use Euclid's Lemma to show that $3^{1/5}$ and $5^{1/3}$ are both irrational.

Solution:
a) Eulid's Lemma (Euclid's *Elements*, Proposition IX.20): Let p be a prime number, and let $a, b \in \mathbb{Z}$. If $p \mid ab$, then $p \mid a$ or $p \mid b$. For future use list the strengthening that we get by applying induction: if $p \mid a_1 \cdots a_n$ then $p \mid a_i$ for some i.
b) Seeking a contradiction, suppose $3^{1/5}$ is rational: then there are nonzero integers a, b, with no common factor, such that

$$3^{1/5} = \frac{a}{b}.$$

Raising both sides to the fifth power and clearing denominators, we get

$$a^5 = 3b^5.$$

Thus $3 \mid a^5 = a \cdots a$; since 3 is prime, (the small generalization above of) Euclid's Lemma implies that $3 \mid a$: so $a = 3A$ for some $A \in \mathbb{Z}$. Thus

$$3^5A^5 = (3A)^5 = a^5 = 3b^5,$$

so

$$b^5 = 3^4A^5.$$

It follows that $3^4 \mid b^5$ and as above that $3 \mid b$. This contradicts our assumption that a and b have no common factor greater than 1 and completes the proof.

The argument for $5^{1/3}$ is extremely similar, and I leave it to you.

2) Let $x, y \in \mathbb{Z}$, and suppose that x is of the form $9k + 3$ for some integer k.
a) Show that $2x^2 + 54y$ is divisible by 9.
b) Show that $2x^2 + 54y$ is not divisible by 27.

Solution: a) We have

$$2x^2 + 54y = 2(9k + 3)^2 + 54y = 2 \cdot 9^2k^2 + 2 \cdot 2 \cdot 3 \cdot 9k + 2 \cdot 3^2 + 54y$$

$$= 9(2 \cdot 9k^2 + 12k + 2 + 6y).$$

Since $2 \cdot 9k^2 + 12k + 2 + 6y \in \mathbb{Z}$, this shows that $9 \mid 2x^2 + 54y$.
b) Looking back at the same calculation, it gives

$$2x^2 + 54y = 27(6k^2 + 4k + 2y) + 18.$$

Date: March 20, 2016.

So, seeking a contradiction, suppose $27 \mid 2x^2 + 54y$, i.e., $2x^2 + 54y = 27A$ for some $A \in \mathbb{Z}$. Then

$$27A = 2x^2 + 54y = 27(6k^2 + 4k + 2y) + 18,$$

so

$$18 = 27(A - (6k^2 + 4k + 2y))$$

and thus $27 \mid 18$. But it does not: contradiction!

3) Let $x \in \mathbb{Z}$. Prove or disprove each of the following statements:
a) If $4 \mid x^2$, then $4 \mid x$.
b) If $5 \mid x^2$, then $5 \mid x$.
c) If $6 \mid x^2$ then $6 \mid x$.

Solution:
a) Disprove: if $x = 2$ then $x^2 = 4$, and we have $4 \mid x^2$ and $4 \nmid x$.
b) This is true, and it follows from Euclid's Lemma for $p = 5$, a case we have already done. It's not much trouble to reproduce the diagonal of the multiplication table modulo 5: if $x \in \mathbb{Z}$, then $x \equiv 0, 1, 2, 3, 4 \pmod 5$. We find:
• If $x \equiv 0 \pmod 5$ then $x^2 \equiv 0^2 = 0 \pmod 5$,
• If $x \equiv 1 \pmod 5$ then $x^2 \equiv 1^2 = 1 \pmod 5$,
• If $x \equiv 2 \pmod 5$ then $x^2 \equiv 2^2 = 4 \pmod 5$,
• If $x \equiv 3 \pmod 5$ then $x^2 \equiv 3^2 = 9 \equiv 4 \pmod 5$,
• If $x \equiv 4 \pmod 5$ then $x^2 \equiv 4^2 = 16 \equiv 1 \pmod 5$.
Thus if $x^2 \equiv 0 \pmod 5$ then $x \equiv 0 \pmod 5$. In other words, if $5 \mid x^2$ then $5 \mid x$.

c) This is true. Again we've seen it before, and again I reproduce the diagonal of the modulo 6 multiplication table:
• If $x \equiv 0 \pmod 6$, then $x^2 \equiv 0^2 = 0 \pmod 6$,
• If $x \equiv 1 \pmod 6$, then $x^2 \equiv 1^2 = 1 \pmod 6$,
• If $x \equiv 2 \pmod 6$, then $x^2 \equiv 2^2 = 4 \pmod 6$,
• If $x \equiv 3 \pmod 6$, then $x^2 \equiv 3^2 = 9 \equiv 3 \pmod 6$,
• If $x \equiv 4 \pmod 6$, then $x^2 \equiv 4^2 = 16 \equiv 4 \pmod 6$,
• If $x \equiv 5 \pmod 6$, then $x^2 \equiv 5^2 = 25 \equiv 1 \pmod 6$.
Thus if $x^2 \equiv 0 \pmod 6$ then $x \equiv 0 \pmod 6$. In other words, if $6 \mid x^2$ then $6 \mid x$.

4) Let $r \neq 1$ be a real number. Show that for all $n \in \mathbb{Z}^+$, $1 + r + \ldots + r^n = \frac{r^{n+1}-1}{r-1}$.

First Solution: We show this by induction on n.
Base Case ($n = 1$): We have $\frac{r^2-1}{r-1} = \frac{(r+1)(r-1)}{r-1} = r + 1 = 1 + r$.
Induction Step: Let $n \in \mathbb{Z}^+$ and suppose that

$$1 + r + \ldots + r^n = \frac{r^{n+1} - 1}{r - 1}.$$

Then

$$1 + r + \ldots + r^{n+1} = (1 + r + \ldots + r^n) + r^{n+1} \stackrel{\text{IH}}{=} \frac{r^{n+1} - 1}{r - 1} + r^{n+1}$$

$$= \frac{r^{n+1} - 1 + (r - 1)(r^{n+1})}{r - 1} = \frac{r^{n+1} - 1 + r^{n+2} - r^{n+1}}{r - 1}$$

$$= \frac{r^{n+2}-1}{r-1}.$$

Second Solution: Let

(1) $$S_n = 1 + \ldots + r + r^n.$$

Multiplying (1) by r we get

(2) $$rS_n = r + \ldots + r^n + r^{n+1},$$

and subtracting (1) from (2) we get

$$(r-1)S_n = r^{n+1} - 1$$

and thus

$$S_n = \frac{r^{n+1}-1}{r-1}.$$

Moral: Many of the things that Superman can do can be done by ordinary people...perhaps with a bit more human ingenuity. (–Lex Luthor?)

5) Consider the following statement: for all $n \in \mathbb{Z}^+$, $3 \mid n^3 + 2n$.
a) Prove the statement using congruences.
b) Prove the statement using induction.

Solution:
a) In the language of congruences, we must show: for all $n \in \mathbb{Z}$ we have $n^3 + 2n \equiv 0 \pmod 3$. The idea is that the value of $n^3 + 2n$ modulo 3 depends only on the value of n modulo 3, so it's enough to verify the congruence for $n = 0, 1, 2$. So:
- $0^3 + 2 \cdot 0 = 0 \equiv 0 \pmod 3$
- $1^3 + 2 \cdot 1 = 3 \equiv 0 \pmod 3$
- $2^3 + 2 \cdot 2 = 12 \equiv 0 \pmod 3$.

b) As instructed, we proceed by induction on n.
Base Case ($n = 1$): We have $1^3 + 2 \cdot 1 = 3$ is divisible by 3.
Induction Step: let $n \in \mathbb{Z}^+$ and suppose that $n^3 + 2n$ is divisible by 3, so $n^3 + 2n = 3A$ for some $A \in \mathbb{Z}$. Then

$$(n+1)^3+2(n+1) = n^3+3n^2+3n+1+2n+2 = (n^3+2n)+(3n^2+3n+3) = 3(A+n^2+n+1).$$

6) A student has been asked to prove: $\forall x \in \mathbb{Z}, P(x) \implies Q(x)$.[1] For each of the following openers, comment on the proof technique, or explain why it is not a valid proof technique.

Example: "Let $x \in S$, and suppose $P(x)$ is true."
Comment: This is the beginning of a direct proof.

a) "Let $x \in S$, and suppose $P(x)$ is false."
b) "Let $x \in S$, and suppose that $Q(x)$ is true."
c) "Let $x \in S$, and suppose $Q(x)$ is false."
d) "Let $x = 1$. Then" [the student shows that $P(1)$ is true and $Q(1)$ is true].
e) "Let $x = 2$. Then" [the student shows that $P(2)$ is false and $Q(2)$ is false].

[1]Here $P(x)$ and $Q(x)$ are sentences involving an arbitrary integer x.

f) "Let $x = 3$. Then" [the student shows that $P(3)$ is true and $Q(3)$ is false].
g) Let $x \in S$, and suppose that $P(x)$ is true and $Q(x)$ is false.

Solution:
a) Negating the consequence is a very strange way to begin a proof. It could only succeed if the implication is trivially true: i.e., if $Q(x)$ is true for all $x \in S$ independently of the truth or falsity of $P(x)$. Don't count on that! But even if that is the case, assuming that $P(x)$ is false is not needed. So there is never a good reason to begin a proof in this way.

b) Here we have assumed what we are trying to prove. **This is the worst mistake in all of mathematics!** Even the nicest of instructors will have to give the student zero points.

c) This is the beginning of a proof by contrapositive.
d) Unless $S = \{1\}$, this could be part of a proof but not the whole thing. If e.g. $S = \mathbb{Z}^+$ and this is the entire proof then this is another terrible mistake: proof of a universally quantified statement by exhibiting a single example. However, let's not be too critical. Many times in order to prove something for all $x \in S$ one needs to handle certain cases separately: perhaps the student begins with $x = 1$ and then goes on to treat an arbitrary element of $S \setminus \{1\}$. So it could be fine...
e) If $P(2)$ is false, then $P(2) \implies Q(2)$ holds vacuously, so...why go to the trouble of showing that $Q(2)$ is false. This is not *wrong* yet (though it is certainly not a complete proof unless $S = \{2\}$)...but it does not inspire confidence.
f) If the argument is correct then the student has **disproved** the statement. Disturbing, perhaps, but not the student's fault. (Maybe there was an html issue?)
g) This is the beginning of a proof by contradiction.

7) a) State the principle of mathematical induction as it applies to subsets of $\mathbb{Z}^+$ and also as a proof technique.
b) True or false: Suppose that for $P(x)$ is an open sentence with domain the real numbers. Then it is simply not possible to use mathematical induction to show that for all $x \in \mathbb{R}$, $P(x)$ holds.

Solution:
a) The principle of mathematical induction for sets is: let $S \subset \mathbb{Z}^+$ and suppose that:
(MI1) $1 \in S$, and
(MI2) For all $n \in \mathbb{Z}^+$, $n \in S \implies n + 1 \in S$.
Then $S = \mathbb{Z}^+$.
The Principle of Mathematical Induction as a proof technique is: let $P(n)$ be an open sentence with domain $\mathbb{Z}^+$. If we can show:
(Base Case) $P(1)$ is true and
(Induction Step) For all $n \in \mathbb{Z}^+$, $P(n) \implies P(n + 1)$,
then it follows that $P(n)$ is true for all $n \in \mathbb{Z}^+$. (The point here is that one can define S to be the set of all positive integers n for which $P(n)$ holds, and by appealing to the above principle for sets we get $S = \mathbb{Z}^+$, which means $P(n)$ holds for all $n \in \mathbb{Z}^+$.

b) True. For any integer N, let $\mathbb{Z}^{\geq N} = \{n \in \mathbb{Z} \mid n \geq N\}$ be the set of integers greater than or equal to N. Then mathematical induction can be straightforwardly modified to give a technique for proving that an open sentence $P(n)$ holds for all integers $n \geq N$: just replace the base case by $n = N$ and in the induction step assume $n \geq N$. However one cannot use induction to show statements $P(x)$ for $x \in \mathbb{R}$.

Addendum: Just so that you don't do some internet searching and decide that I am being dishonest with you: there *is* a proof technique which can be applied to show statements $P(x)$ for $x \in \mathbb{R}$ and which has much of the spirit of mathematical induction. I call this technique **real induction** and have written an article about it.

`http://math.uga.edu/~pete/instructors_guide_shorter.pdf.`

But one should have mathematical induction down cold before studying such jazz riffs on it.

8) a) Show: $n! > 2^n$ for all $n \geq 4$.
b) Show: $n! > 3^n$ for all $n \geq 7$.
(You may use that $7! = 5040$ and $3^7 = 2187$.)

Solution:
a) By induction on n.
Base Case ($n = 4$): We have $4! = 24 > 16 = 2^4$.
Induction Step: Let $n \geq 4$ and suppose $n! > 2^n$. Since $n \geq 4$, we have

$$n + 1 \geq 5 > 2,$$

and thus

$$(n + 1)! = (n + 1)n! \stackrel{\text{IH}}{>} (n + 1)2^n > 2 \cdot 2^n = 2^{n+1}.$$

b) By induction on n.
Base Case ($n = 7$): We have $7! = 5040 > 2187 = 3^7$.
Induction Step: Let $n \geq 7$ and suppose $n! > 3^n$. Since $n \geq 7$ we have

$$n + 1 \geq 8 > 3,$$

and thus

$$(n + 1)! = (n + 1)n! \stackrel{\text{IH}}{>} (n + 1)3^n > 3 \cdot 3^n = 3^{n+1}.$$

9) Show: for all integers $n \geq 0$, we have $\int_0^\infty x^n e^{-x} dx = n!$

Solution: Please see Proposition 16 on page 14 of

`http://alpha.math.uga.edu/~pete/3200induction.pdf`.

10) Let A be a set. Prove or disprove: if for every set B, $A \setminus B = \varnothing$, then $A = \varnothing$.

Solution: Proof: Taking $B = \varnothing$ gives $\varnothing = A \setminus \varnothing = A$.
(What? There can be easy questions!)

11) Prove or disprove:
a) For all rational numbers a and b, $a + b$ and ab are both rational.
b) For all irrational (real) numbers a and b, $a + b$ is irrational.
c) For all irrational (real) numbers a and b, $a + b$ is rational.
d) For all irrational (real) numbers a and b, ab is irrational.
e) For all irrational (real) numbers a and b, ab is rational.

Solution:
a) Proof: write $a = \frac{p}{q}$ and $b = \frac{r}{s}$ with $p, q, r, s \in \mathbb{Z}$ and $r, s \neq 0$. Then

$$a + b = \frac{p}{q} + \frac{r}{s} = \frac{ps + qr}{qs} \in \mathbb{Q},$$

$$ab = \frac{p}{q}\frac{r}{s} = \frac{pr}{qs} \in \mathbb{Q}.$$

b) Disproof: take $a = \sqrt{2}$ and $b = -\sqrt{2}$. Then a, b are irrational and $a + b = 0 \in \mathbb{Q}$.
c) Disproof: take $a = b = \sqrt{2}$. Then a, b are irrational and $a + b = 2\sqrt{2}$ is irrational. (If $2\sqrt{2} = \frac{p}{q}$ were rational, then $\sqrt{2} = \frac{p}{2q}$ would be rational..and we know it isn't.)
d) Disproof: take $a = b = \sqrt{2}$. Then a, b are irrational and $ab = \sqrt{2}\sqrt{2} = 2 \in \mathbb{Q}$.
e) Disproof: take $a = \sqrt{2}$, $b = \sqrt{3}$. Then a, b are both irrational and $ab = \sqrt{2}\sqrt{3} = \sqrt{6}$ which is (as we've seen at least twice now) irrational.