PRACTICE PROBLEMS FOR MATH 109 MIDTERM 2. You may work on these in addition to reviewing HW problems to help prepare for midterm 2.

1. Prove that if \( n \) is a perfect square, then \( n = 5q, n = 5q + 1, \) or \( n = 5q + 4 \) for some \( q \in \mathbb{Z} \). 

**HINT:** See the proof of Proposition 15.2.1. 

**Ans.** Suppose that \( n \) is a perfect square. Then there exists \( a \in \mathbb{Z} \) such that \( n = a^2 \). By the division theorem, there exists \( k \in \mathbb{Z} \) such that either:

- (a) \( a = 5k \), in which case \( n = 5(5k^2) \).
- (b) \( a = 5k + 1 \), in which case \( n = 5(5k^2 + 2k) + 1 \).
- (c) \( a = 5k + 2 \), in which case \( n = 5(5k^2 + 4k) + 4 \).
- (d) \( a = 5k + 3 \), in which case \( n = 5(5k^2 + 6k + 1) + 4 \).
- (e) \( a = 5k + 4 \), in which case \( n = 5(5k^2 + 8k + 3) + 1 \).

The result follows since the only remainders (after dividing by 5) are 0, 1, and 4.

2. Prove that if \( d = 6p + 2 \) for some \( p \in \mathbb{Z} \) or if \( d = 6q + 5 \) for some \( q \in \mathbb{Z} \), then \( d \) is not a perfect square.

**Ans.** Suppose that \( n \) is a perfect square. Then there exists \( a \in \mathbb{Z} \) such that \( n = a^2 \). By the division theorem, there exists \( k \in \mathbb{Z} \) such that either:

- (a) \( a = 6k \), in which case \( a^2 = 6(6k^2) \).
- (b) \( a = 6k + 1 \), in which case \( a^2 = 6(6k^2 + 2k) + 1 \).
- (c) \( a = 6k + 2 \), in which case \( a^2 = 6(6k^2 + 4k) + 4 \).
- (d) \( a = 6k + 3 \), in which case \( a^2 = 6(6k^2 + 6k + 1) + 3 \).
- (e) \( a = 6k + 4 \), in which case \( a^2 = 6(6k^2 + 8k + 2) + 4 \).
- (f) \( a = 6k + 5 \), in which case \( a^2 = 6(6k^2 + 10k + 4) + 1 \).

Hence the remainder of a perfect square modulo 6 is 0, 1, 3, or 4. Thus 2 and 5 cannot be remainders.

3. Let \( a \) be a positive integer and let \( p \) be a prime number. Prove that \( a^2 \) is divisible by \( p \) if and only if \( a \) is divisible by \( p \). 

**HINT:** See Exercise 15.2. With this, you can also do Exercise 15.3. 

**Ans.** This was done in class.

4. Let \( p \) be a prime number. Prove that \( \sqrt{p} \) is irrational. 

**HINT:** Using the previous problem, the proof is the same as for proving that \( \sqrt{2} \) is irrational by contradiction.

**Ans.** Follow the hint.

5. Let \( a, q, r \in \mathbb{Z} \) and \( b \in \mathbb{Z}^+ \) be such that \( a = bq + r \). Prove that \( D(b, r) = D(a, b) \). 

**HINT:** See Exercise 16.4. 

**Ans.** Exercise 16.4 proves \( D(b, r) \subseteq D(a, b) \). But then the reverse containment follows from \( r = -bq + a \) by the same logic.

6. Let \( a, b \) and \( c \) be nonzero integers. Prove that if \( a \) and \( b \) are coprime and \( a \) divides \( bc \), then \( a \) divides \( c \). 

**HINT:** See the proof of Theorem 17.3.2. 

**Ans.** \( \exists m, n, ma + nb = 1, \) so \( cma + cnb = c \). Clearly \( a \mid cma \). Since \( a \mid bc, a \mid cnb \). So \( a \mid (cma + cnb), \) i.e., \( a \mid c \).
7. Let \(a, b\) and \(c\) be nonzero integers. Let \(g = \gcd(a, b)\). Prove that if \(a\) divides \(bc\), then \(\frac{a}{g}\) divides \(c\). HINT: Generalize the proof of the previous problem.

**Ans.** \(\exists m, n, ma+nb = g\), so \(cm\frac{a}{g} + n\frac{bc}{g} = c\). Clearly \(\frac{a}{g}\) divides \(cm\frac{a}{g}\). Since \(a|bc\), \(\frac{a}{g}\) divides \(n\frac{bc}{g}\). So \(\frac{a}{g}\) divides \(cm\frac{a}{g} + n\frac{bc}{g}\), i.e., \(\frac{a}{g}\) divides \(c\).

8. Find all integer solutions \((m, n)\) such that \(36m + 24n = 84\). In doing so, derive that this is the complete solution set (don’t just use a formula). HINT: See the proof of Proposition 18.4.1 and the solutions to Examples 18.3.1 and 18.4.2.

**Ans.** \(36m + 24n = 84 \iff 3m + 2n = 7\). One solution (by inspection) is \(m_0 = 1\) and \(n_0 = 2\). General solution is

\[
m = 1 + 2k, \quad n = 2 - 3k, \quad k \in \mathbb{Z}.
\]

9. Let \(m \in \mathbb{N}\). Prove: If \(a_1 \equiv a_2 \mod m\) and \(b_1 \equiv b_2 \mod m\), then

(a) \(a_1 + b_1 \equiv a_2 + b_2 \mod m\).

(b) \(a_1b_1 \equiv a_2b_2 \mod m\). HINT: See the proof of Proposition 19.1.3.

**Ans.** (b) was done in class.

10. Prove, using the definition of congruence and using properties of division, that \(15a \equiv 15b \mod 39\) if and only if \(a \equiv b \mod 13\). HINT: Apply Proposition 19.3.1.

**Ans.** \(15a \equiv 15b \mod 39 \iff a \equiv b \mod \frac{39}{\gcd(15,39)}\). Done, since \(\frac{39}{\gcd(15,39)} = 13\).

11. Find all solutions to the equation \(6x \equiv 21 \mod 15\). And, how many solutions are there modulo 15? HINT: See Example 19.3.4.

**Ans.** \(6x \equiv 21 \mod 15 \iff 2x \equiv 7 \mod 5 \iff 2x \equiv 12 \mod 5 \iff x \equiv 6 \mod 5\). Solution set \(= \{6 + 5k : k \in \mathbb{Z}\}\). 3 solutions modulo 15.

12. Let \(r_6 : \mathbb{Z} \to R_6\) be the remainder map. Prove that if \(a, b \in \mathbb{Z}\) satisfy \(r_6(a) = r_6(b)\), then \(r_6(a^2) = r_6(b^2)\). HINT: Use the equality \(a^2 - b^2 = (a + b)(a - b)\) and Proposition 19.2.4.

**Ans.** \(r_6(a) = r_6(b) \Rightarrow 6|a - b \Rightarrow 6|(a + b)(a - b) \Rightarrow 6|(a^2 - b^2) \Rightarrow r_6(a^2) = r_6(b^2)\).

13. Prove that if \(a \in \mathbb{Z}\), then there exists an integer \(c\) with \(0 \leq c < 6\) such that \(r_6(a) = r_6(c)\). HINT: Use the division theorem and Proposition 19.2.4.

**Ans.** Another hint: \(c\) is the remainder.

14. It is a fact that \(r_6(0^2) = 0\), \(r_6(1^2) = r_6(5^2) = 1\), \(r_6(2^2) = r_6(4^2) = 4\), \(r_6(3^2) = 3\). Using this, prove that if \(a \in \mathbb{Z}\), then \(r_6(a^2) \in \{0, 1, 3, 4\}\). REMARK: This is related to Problem 2 above.

**Ans.** The solution to Problem 2 yields the answer.

15. *In your own words, prove the following statement.* Two integers are congruent modulo 17 if and only if they have the same remainder after being divided by 17. HINT: This is a special case of Proposition 19.2.4.

**Ans.** \(a \equiv b \mod 17 \iff 17|(a - b) \iff 17|(r_{17}(a) - r_{17}(b)) \iff r_{17}(a) = r_{17}(b)\). The last \(\iff\) uses the fact that

\[-17 < r_{17}(a) - r_{17}(b) < 17,\]
which is true since $r_{17}(a) \geq 0$ and $r_{17}(b) < 17$ imply $r_{17}(a) - r_{17}(b) > -17$, whereas $r_{17}(a) < 17$ and $r_{17}(b) \geq 0$ imply $r_{17}(a) - r_{17}(b) < 17$. In particular, $17 \mid (r_{17}(a) - r_{17}(b)) \Rightarrow -1 < \frac{r_{17}(a) - r_{17}(b)}{17} < 1$ and $\frac{r_{17}(a) - r_{17}(b)}{17}$ is an integer. Hence $\frac{r_{17}(a) - r_{17}(b)}{17} = 0$.

16. Do all the homework problems for HW 5, HW 6, and HW 7.