Selected solutions to Homework # 6

1. #2 in Appendix D.
Define a relation on \( \mathbb{Q} \) via \( r \sim s \) if and only if \( r - s \in \mathbb{Z} \). Prove that \( \sim \) is an equivalence relation.

Proof: We need to show three properties hold:
1. Reflexive: show that \( r \sim r \) for every \( r \in \mathbb{Q} \). This is true since \( r - r = 0 \in \mathbb{Z} \).
2. Symmetric: show that if \( r \sim s \), then \( s \sim r \). Suppose that \( r \sim s \). Thus \( r - s \in \mathbb{Z} \). If \( a \in \mathbb{Z} \), then \( -a \in \mathbb{Z} \). So, \( -(r - s) = s - r \in \mathbb{Z} \). Therefore, \( s \sim r \).
3. Transitive: show that if \( r \sim s \) and \( s \sim t \), then \( r \sim t \). Suppose that \( r \sim s \) and \( s \sim t \). Then \( (r - s) + (s - t) \) are integers. This implies that \( (r - s) + (s - t) \) is an integer. Therefore \( r - t \in \mathbb{Z} \) and so \( r \sim t \).

Having checked the defining properties, we have shown that \( \sim \) is an equivalence relation.

2. #20 in Section 1.3
We discussed this problem in class on 01/28/11.

3. #2 in Section 2.1
(a) We discussed this problem in class on 01/26/11.
(b) If \( r \equiv 3 \pmod{10} \) and \( s \equiv -7 \pmod{10} \), then what is \( 2r + 3s \) congruent to modulo 10?

We expect that since \( 2 \times 3 = 6 \) and since \( 3 \times (-7) = -21 \equiv (-1) \pmod{10} \), we should have that \( 2r + 3s \) is congruent to \( 6 - 1 = 5 \) modulo 10.

Claim: \( 2r + 3s \equiv 5 \pmod{10} \).

Proof: We are given that \( (r - 3) = 10k \) and \( (s - (-7)) = 10l \) for some integers \( k \) and \( l \). Solving for \( r \) and \( s \) and multiplying by 2 and 3 respectively, we have

\[
2r + 3s = 2(10k + 3) + 3(10l - 7) = 10 \cdot 2k + 6 + 10 \cdot 3l - 21 = 10(2k + 3l) - 15.
\]

Since \( -15 = -2(10) + 5 \), \( 2r + 3s = 10(2k + 3l - 2) + 5 \). Therefore,

\[
(2r + 3s) - 5 = 10(2k + 3l - 2).
\]
So, by definition, $2r + 3s$ is congruent to 5 modulo 10. Q.E.D.

Alternate Proof: Use the properties of Theorem 2.2. and compute: $2r \equiv 2(3)(\text{mod } 10)$, $3s \equiv 3(-7)(\text{mod } 10)$. Therefore $2r + 3s \equiv (6 - 21)(\text{mod } 10)$. And $-15 \equiv 5(\text{mod } 10)$.

You should compute freely as in the “Alternate Proof” above. The point of Theorem 2.2 is that we do not need to write tedious proofs as in the first “Proof” that I wrote above. Rather, you can perform arithmetic as usual and reduce each of the calculations modulo $n$ at any stage of your computation.

4. #12 in Section 2.1

Which of the following congruences have solutions:

(a) $x^2 \equiv 1(\text{mod } 3)$.
   
   Let $x = 2$. This is a solution since $2^2 = 4 \equiv 1(\text{mod } 3)$.

(b) $x^2 \equiv 2(\text{mod } 7)$.
   
   Let $x = 3$. Then $x^2$ is congruent to 2 modulo 7.

(c) $x^2 \equiv 3(\text{mod } 11)$.
   
   Let $x = 5$. Then $x^2$ is congruent to 3 modulo 11.

5. #19 in Section 2.1

(a) Prove or disprove: if $a^2$ and $b^2$ are congruent modulo $n$, then $a$ is congruent to either $b$ or $-b$ modulo $n$.

   This is false: take $n = 4$, $a = 2$, $b = 4$. Then $a^2 = 4$ and $b^2 = 16$, and these are congruent modulo 4. But 2 is not congruent to 0 (or “minus zero”).

(b) As above, but assume $n$ is prime.

   This is true. I will write $p$ in place of $n$ so that we remember that $n = p$ is prime.

   Since $a^2$ and $b^2$ are congruent modulo $p$, we have that $a^2 - b^2 = kp$ for some $k \in \mathbb{Z}$. Factoring, we have that $(a - b)(a + b) = kp$. Since $p$ is prime, we have (by Theorem 1.8) that either $p$ divides $(a - b)$ or $p$ divides $(a+b)$. In other words, either $a \equiv b(\text{mod } p)$ or $a \equiv -b(\text{mod } p)$.

   The proof above is worth studying. It shows that Theorem 1.8 can be very useful. In fact, when we discuss rings in chapter 3, we will see that the theorem 1.8 is used to define the notion of a prime element in a more general setting. Here is a preview: we can study arithmetic
using polynomials with integer coefficients. If we think of polynomials as “numbers”, what does it mean for a polynomial to be prime?

6. Find the unique solution to

\[ r \equiv (42)^{17} \pmod{5} \]

such that \(0 \leq r < 5\).

We discussed this problem in class on 01/26/11.