Math 345 – Monday 9/18/17

Exercise 13. Consider positive integers a, b, and c.

(a) Suppose $\gcd(a, b) = 1$.
   (i) Show that if a divides the product bc, then a must divide c.
   (ii) Show that if a and b both divide c, then ab must also divide c.

(b) Give examples of a, b, and c where $\gcd(a, b) \neq 1$ and...
   (i) a divides the product bc, but a does not divide c;
   (ii) a and b both divide c, but ab does not divide c.

Exercise 14. Let s and t be odd integers with $s > t \geq 1$ and $\gcd(s, t) = 1$. Prove that the three numbers

$$st, \qquad \frac{s^2 - t^2}{2}, \qquad \text{and} \qquad \frac{s^2 + t^2}{2}$$

are pairwise relatively prime (i.e. each pair of them is relatively prime). This fact was needed to complete the proof of the Pythagorean triples theorem (Theorem 2.1 on page 17). [Hint. Assume that there is a common prime factor and use the fact (Lemma 7.1) that if a prime divides a product, then it divides one of the factors.]

Exercise 15. Group the numbers $-10 \leq i \leq 10$ into sets according to which numbers are pairwise congruent modulo 4. [You should have 4 sets of roughly the same size.]

Exercise 16. Fix $n \geq 1$.

(a) Prove that congruence is an equivalence relation by showing
   (i) reflexivity: $a \equiv a \pmod{n}$ for all $a \in \mathbb{Z}$;
   (ii) symmetry: if $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$; and
   (iii) transitivity: if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.

(b) Suppose $a_1 \equiv b_1 \pmod{n}$ and $a_2 \equiv b_2 \pmod{n}$.
   (i) Show that $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$ and $a_1 - a_2 \equiv b_1 - b_2 \pmod{n}$
   (ii) Show that $a_1 a_2 \equiv b_1 b_2 \pmod{n}$.

(c) Division.
   (i) Give an example of a, b, c, and n, with $c \not\equiv 0 \pmod{n}$, where

$$ac \equiv bc \pmod{n}, \qquad \text{but} \qquad a \not\equiv b \pmod{n}.$$

   (ii) Show that if $\gcd(c, n) = 1$, then

$$ac \equiv bc \pmod{n} \qquad \text{implies} \qquad a \equiv b \pmod{n}.$$