MAT 312/AMS 351
Applied Abstract Algebra
Midterm 1 – Solutions

1. (a) Calculate the multiplicative inverse of 11 mod 173.

   Apply the Euclidean Algorithm:

   $$173 = 15 \times 11 + 8$$
   $$11 = 1 \times 8 + 3$$
   $$8 = 2 \times 3 + 2$$
   $$3 = 1 \times 2 + 1$$

   and now backwards, since $(173, 11) = 1$:

   $$1 = 3 - 2$$
   $$1 = 3 - (8 - 2 \times 3) = -8 + 3 \times 3$$
   $$1 = -8 + 3(11 - 1 \times 8) = 3 \times 11 - 4 \times 8$$
   $$1 = 3 \times 11 - 4(173 - 15 \times 11) = 63 \times 11 - 4 \times 173$$

   so the answer is 63.

   (b) Solve $11x \equiv 15 \bmod 173$.

   Multiply the equation by the inverse of 11:

   $$63 \times 11x \equiv 63 \times 15 \bmod 173$$

   $$x \equiv 945 \equiv 80 \bmod 173.$$

2. (30 points)

   (a) Find the greatest common divisor d of 935 and 272.

   Euclidean algorithm:

   $$935 = 3 \times 272 + 119$$
   $$272 = 2 \times 119 + 34$$
   $$119 = 3 \times 34 + 17$$
   $$34 = 2 \times 17$$

   so $(935, 272) = 17$

(b) Express d as an integral linear combination: $d = s\cdot 935 + t\cdot 272$. run the algorithm backwards:

$$17 = 119 - 3 \times 34$$
$$17 = 119 - 3(272 - 2 \times 119) = -3 \times 272 + 7 \times 119$$
$$17 = -3 \times 272 + 7(935 - 3 \times 272) = -24 \times 272 + 7 \times 935.$$

(c) Solve $272x \equiv 34 \mod 935$.

The equations has solutions because 34 is a multiple of $(935, 272) = 17$.
First divide through by 17 and solve

$$16x \equiv 2 \mod 55.$$

The inverse of 16 mod 55 is 31; this number satisfies $16 \times 31 \equiv 1 \mod 55$ so $2 \times 31 = 62$ satisfies $16 \times 62 \equiv 2 \mod 55$; this can be simplified to $7 = 62 - 55$:

$$16 \times 7 = 112 \equiv 2 \mod 55.$$

Now multiplying by 17 gives a solution to our original equation:

$$16 \times 17 \times 7 \equiv 2 \times 17 \mod 55 \times 17$$

or

$$272 \times 7 \equiv 34 \mod 935.$$

There are 16 other solutions:

$$7 + 55, 7 + 2 \times 55, \ldots, 7 + 16 \times 55$$

since these numbers are all different $\mod 935 = 17 \times 55$, and

$$272 \times (7 + k \times 55) \equiv 34 + k \times 272 \times 55 \equiv 34 + k \times 16 \times 17 \times 55 \equiv 34 + 16k \times 935 \equiv 34 \mod 935.$$

3. (20 points) Prove (by induction, or otherwise) that

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2$$

i.e. that the sum of the first n odd numbers is equal to n^2.

Let $P(n)$ be the statement $1 + 3 + 5 + \cdots + (2n - 1) = n^2$.
$P(1)$ is true, since $1 = 1$.
We show $P(k) \Rightarrow P(k + 1)$ for $k \geq 1$. By induction, this completes the proof.
Start with $P(k)$:

$$1 + 3 + 5 + \cdots + (2k - 1) = k^2$$

add $2k + 1$ to both sides

$$1 + 3 + 5 + \cdots + (2k - 1) + (2k + 1) = k^2 + 2k + 1 = (k + 1)^2$$

which is $P(k + 1)$.

4. (10 points) Give numbers a and b such that 15 divides ab but does not divide either a or b.

   Simplest example: $a = 3, b = 5$.

5. (20 points) Solve the system

$$x \equiv 4 \bmod 17$$

$$x \equiv 1 \bmod 13.$$

   The moduli are relatively prime, so we can always find solutions. First write $1 = s \times 17 + t \times 13$:

$$17 = 13 + 4$$

$$13 = 3 \times 4 + 1$$

   so

$$1 = 13 - 3 \times 4 = 13 - 3 \times (17 - 13) = 4 \times 13 - 3 \times 17,$$

   which means

$$4 \times 13 \equiv 1 \bmod 17, \qquad (-3) \times 17 \equiv 1 \bmod 13$$

   Then notice that

$$1 \times [(-3) \times 17] + 4 \times [4 \times 13]$$

   is a solution of both equations. This number is $16 \times 13 - 3 \times 17 = 157$. Any other solution comes from adding to 157 a multiple of 13×17.