Math 445 — Problem Set #1
Due: Friday, September 1 by 7 pm, on Canvas

Instructions: You are encouraged to work together on these problems, but each student should hand in their own final draft, written in a way that indicates their individual understanding of the solutions. Never submit something for grading that you do not completely understand.

If you do work with others, I ask that you write something along the top like "I collaborated with Steven Smale on problems 1 and 3". If you use a reference, indicate so clearly in your solutions. In short, be intellectually honest at all times.

Please write neatly, using complete sentences and correct punctuation. Label the problems clearly.

(1) Which of the following are true?
  (a) $10 \equiv 45 \pmod 5$
  (b) $19 \equiv 2 \pmod{12}$
  (c) $150974 \equiv 6 \pmod 8$.

> (a) This is true, since 5 divides $45 - 10 = 35$.
> (b) This is false, since 12 does not divide $19 - 2$.
> (c) This is true, since 8 divides $150974 - 6 = 150966$.

(2) Let m, m', n, n', K be integers with $K > 0$. Prove that if

$$m \equiv m' \pmod K \text{ and } n \equiv n' \pmod K$$

then

$$m + n \equiv m' + n' \pmod K \text{ and } mn \equiv m'n' \pmod K.$$

> By hypothesis, we can write $m - m' = aK$ and $n - n' = bK$ for some integers a, b. Then
>
> $$(m + n) - (m' + n') = (m - m') + (n - n') = aK + bK = (a + b)K,$$
>
> so $m + n \equiv m' + n' \pmod K$, and
>
> $$mn - m'n' = mn - m'n + m'n - m'n' = (m - m')n + m'(n - n') = naK + m'bK = (na + m'b)K,$$
>
> so $mn \equiv m'n' \pmod K$.

(3) Divisibility tests and congruences:
  (a) Show that any natural number is congruent modulo 4 to the two digit number (in base ten) that corresponds to its last two digits. Use this to show that a number is divisible by 4 if and only if its last "two digit part" is divisible by 4.
  (b) Show that any natural number is congruent modulo 8 to the three digit number (in base ten) that corresponds to its last three digits. Use[1] this to show that a number is divisible by 8 if and only if its "last three digit part" is divisible by 8.

[1]The step from the first sentence to the second sentence is similar to that in part (a); once you are convinced of this, you can just say this instead of repeating the argument.

(c) Show[2] that any natural number is congruent modulo 3 to the sum of its digits. Use this to show that a number is divisible by 3 if and only the sum of its digits is divisible by 3.

(d) Show that any natural number is congruent modulo 9 to the sum of its digits. Use this to show that a number is divisible by 9 if and only the sum of its digits is divisible by 9.

(e) Show that any natural number is congruent modulo 11 to the alternating sum of its digits, i.e.

$$\text{1s digit} - \text{10s digit} + \text{100s digit} \pm \cdots .$$

Use this to show that a number is divisible by 11 if and only the alternating sum of its digits is divisible by 11.

(a) Let n be the natural number with digit expansion $a_t a_{t-1} \cdots a_1 a_0$, so $n = 10^t a_t + 10^{t-1} a_{t-1} + \cdots + 10a_1 + a_0$. Then the two digit number n' that corresponds to the last two digits is $10a_1 + a_0$. We compute

$$\begin{aligned} n - n' &= (10^t a_t + 10^{t-1} a_{t-1} + \cdots + 10a_1 + a_0) - (10a_1 + a_0) \\ &= 10^t a_t + 10^{t-1} a_{t-1} + \cdots + 10^2 a_2 = 10^2 (10^{t-2} a_t + 10^{t-3} a_{t-1} + \cdots + a_2) \end{aligned}$$

is a multiple of 100, and hence of 4. This shows the first statement. Then $4|n$ if and only if $n \equiv 0 \pmod 4$ if and only if $n' \equiv 0 \pmod 4$ if and only if $4|n'$.

(b) Let n be as above. Then the three digit number n' that corresponds to the last three digits is $10^2 a_2 + 10a_1 + a_0$. We compute

$$\begin{aligned} n - n' &= (10^t a_t + 10^{t-1} a_{t-1} + \cdots + 10a_1 + a_0) - (10^2 a_2 + 10a_1 + a_0) \\ &= 10^t a_t + 10^{t-1} a_{t-1} + \cdots + 10^3 a_3 = 10^3 (10^{t-3} a_t + 10^{t-4} a_{t-1} + \cdots + a_3) \end{aligned}$$

is a multiple of 1000, and hence of 8. This shows the first statement. The second follows form the first as in (a).

(c) We have $10 \equiv 1 \pmod 3$, so, using problem #2, $10^k \equiv 1^k \equiv 1 \pmod 3$ for all k. Then, again using problem #2, $n = 10^t a_t + 10^{t-1} a_{t-1} + \cdots + 10a_1 + a_0$ is congruent to $a^t + a_{t-1} + \cdots + a_1 + a_0$ modulo 3.

(d) We have $10 \equiv 1 \pmod 9$, so just as above, $n = 10^t a_t + 10^{t-1} a_{t-1} + \cdots + 10a_1 + a_0$ is congruent to $a^t + a_{t-1} + \cdots + a_1 + a_0$ modulo 9.

(e) We have $10 \equiv -1 \pmod 1 1$, so using problem #2, $10^k \equiv (-1)^k \pmod 1 1$ for all k. Then $n = 10^t a_t + 10^{t-1} a_{t-1} + \cdots + 10a_1 + a_0$ is congruent to $(-1)^t a^t + (-1)^{t-1} a_{t-1} + \cdots + (-1) a_1 + a_0$ modulo 11.

(4) The number 150974 is a sum of three squares:

$$362^2 + 141^2 + 7^2 = 150974.$$

In this problem we will show that 150975 is *not* a sum of three squares; i.e., there are no integers a, b, c such that

$$a^2 + b^2 + c^2 = 150975.$$

(a) Show that if a is odd, then $a^2 \equiv 1 \pmod 8$.

[2] Hint: Start by showing that $10^k \equiv 1 \pmod 3$ for any k.

(b) Show[3] that if a is even, then either $a^2 \equiv 0 \pmod 8$ or $a^2 \equiv 4 \pmod 8$.
(c) Show that if $n = a^2 + b^2 + c^2$, then $n \equiv 7 \pmod 8$ is impossible.
(d) Conclude that 150975 is not a sum of three squares.

(a) Write $a = 2k+1$. Then $a^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 4k(k+1) + 1$. Since either k is even or $k+1$ is even, $4k(k+1)$ is a multiple of 8, so $a^1 \equiv 1 \pmod 8$.
(b) If $a \equiv 0 \pmod 4$, write $a = 4k$; then $a^2 = 16k^2 \equiv 0 \pmod 8$. If $a \equiv 2 \pmod 4$, write $a = 4k+2$; then $a^2 = 16k^2 + 16k + 4 \equiv 4 \pmod 8$.
(c) We proceed by cases: up to symmetry, mod 8 we have

a^2	b^2	c^2	$a^2 + b^2 + c^2$
4	4	4	4
4	4	1	1
4	4	0	0
4	1	1	6
4	1	0	5
4	0	0	4
1	1	1	3
1	1	0	2
1	0	0	1
0	0	0	0

and 7 is impossible.
(d) 150975 is congruent to 7 modulo 8. If $a^2 + b^2 + c^2 = 150975$, then we would have $a^2 + b^2 + c^2 \equiv 150975 \equiv 7 \pmod 8$, which is impossible.

(5) Let a, b, c be integers. Use prime factorization to show that if a and b have no common prime factor and a divides bc, then a divides c.

Take prime factorizations $a = p_1^{e_1} \cdots p_s^{e_s}$ and $b = q_1^{f_1} \cdots q_t^{f_t}$ for some primes, where the p's and q's are primes with no common value. Suppose that a does not divide c. Then in the prime factorization of c, some p_i occurs with a factor of less than e_i. But in bc, the multiplicity of the prime p_i in the prime factorization is the same as that in c, since p_i does not occur in a. Thus, a does not divide bc.

The remaining problems are only required for Math 845 students, though all are encouraged to think about them.

(6) Recall that the Fibonacci sequence is given by the formula

$$f_{n+2} = f_{n+1} + f_n, \; f_0 = f_1 = 1.$$

For which n is f_n a multiple of 2? A multiple of 4? A multiple of 5?

[3] Hint: Every even number is congreunt to 0 mod 4 or to 2 mod 4.

We compute some values of f_i modulo 2:

$$1, 1, 0, 1, 1, 0, \ldots.$$

Since $f_3 = f_4 = 1$ modulo 2, it follows that $f_n \equiv f_{n+3} \pmod 2$. Using this periodicity, we see that f_n is even if and only if $n \equiv 2 \pmod 3$.

Similarly, modulo 4:

$$1, 1, 2, 3, 1, 0, 1, 1, 2 \ldots.$$

Along similar lines, $f_n \equiv f_{n+6} \pmod 4$, and f_n is a multiple of 4 if and only if $n \equiv 5 \pmod 6$.

And modulo 5:

$$1, 1, 2, 3, 0, 3, 3, 1, 4, 0, 4, 4, 3, 2, 0, 2, 2, 4, 1, 0, 1, 1, 2, \ldots,$$

and f_n is a multiple of 5 if and only if $n \equiv 4, 9, 14, 19 \pmod{20}$, or $n \equiv 4 \pmod 5$.

(7) Find a formula for all of the rational points (x, y) on the hyperbola $x^2 - 2y^2 = 1$.

We have $P = (-1, 0)$ on the hyperbola. The line with slope m through P has formula $y = m(x + 1)$, and meets the hyperbola at a point satisfying

$$x^2 + m^2(x + 1) = 1.$$

We can rewrite as

$$\begin{gathered}(x+1)^2 - 2(x+1) + 1 + m^2(x+1) = 1 \\ (x+1)(1+m^2) - 2 = 0 \\ x = \frac{2}{1+m^2} - 1, \\ y = \frac{2m}{1+m^2}.\end{gathered}$$

Note that if m is rational, then x and y are rational, and if x, y are rational, then $m = \dfrac{y}{x+1}$ is rational as well.

It follows that there is a bijection between rational points on the hyperbola other than P and rational numbers, and in particular, that

$$(x, y) = \left(\frac{2}{1+m^2} - 1, \frac{2m}{1+m^2}\right) \quad m \in \mathbb{Q}$$

gives a formula for all of the rational points on the hyperbola (besides P).