Math 546 Test 1.

This is due on Sunday, September 20 at midnight. You are to work alone in it. You can look up definitions and the statements of theorems we have covered in class. Needless to say (but I will say it anyway) no use of online help sites such as Stack Overflow or Chegg.

Problem 1 (5 points). Show for all positive integers n that $31^n - 1$ is divisible by 6. $\square$

Problem 2 (5 points). Solve the equation $[13]_{67}[x]_{67} = [17]_{67}$ in $\mathbb{Z}_{67}$. $\square$

Problem 3 (5 points). Find the solution to $105x \equiv 21 \pmod{91}$. $\square$

Problem 4 (5 points). For this problem you will need to review that statement of the binomial theorem.

(a) What is the binomial expansion of $(x+y)^7$?

(b) Prove that for all integers a and b that

$$(a+b)^7 \equiv a^7 + b^7 \pmod 7.$$

(It turns out this is true with 7 replaced by any prime, but just do the proof in the case of 7.)

Problem 5 (10 points). Let a, b, and n be positive integers such that $a \mid n$ and $b \mid n$.

(a) Give an example where this holds, but $(ab) \nmid n$. (That is a and b both divide n but the product ab does not divide n.)

(b) Show that if also $\gcd(a,b) = 1$, then $(ab) \mid n$. (That is if a and b both divide n and also $\gcd(a,b) = 1$, then the product ab divides n.) $\square$

Problem 6 (20 points). We start this problem with a couple of examples. If we look at numbers modulo 4, then every integer x is congruent to exactly one of 0, 1, 2, or 3. So if we compute the squares of integer modulo 4 and make a table:

x	0	1	2	3
x^2	0	1	0	1

From this we see that if $n = x^2$ is the square of an integer, then n is congruent to either 0 or 1 modulo 4. Thus if $n \equiv 2 \pmod 4$ or $n \equiv 3 \pmod 4$, then n is not a perfect square. Likewise we can make a table of all the possible values of $x^2 + y^2$ modulo 4:

	0	1	2	3
0	0	1	0	1
1	1	2	1	2
2	0	1	0	1
3	1	2	1	2

In this table for the row labeled 1 and the column labeled 3 the entry is $2 \equiv 1^2 + 3^2 \pmod 4$. From this table we see that if $n \equiv 3 \pmod 4$, then it is impossible to write n as a sum of two perfect squares.

(a) Make a table of the values of $x^2 + xy + y^2$ modulo 3 and use this to explain why that if $n \equiv 2 \pmod 3$, then there are no integers x and y with $n = x^2 + xy + y^2$.

(b) Show there are no integers x and y with $x^3 + xy - y^3 = 10{,}002$. □

Problem 7 (20 points). Let c_0, c_1, c_2, c_3, c_4 be integers with $c_4 \neq 0$ and let

$$f(x) = c_4x^4 + c_3x^3 + c_2x^2 + c_1x + c_0.$$

(a) Let $r = \dfrac{p}{q}$ be a rational number in lowest terms (that is $\gcd(p, q) = 1$) with $f(r) = 0$. Prove that $p \mid c_0$ and $q \mid c_4$.

(b) Show that if n is not a perfect fourth power (that is $n \neq a^4$ for any integer) then $\sqrt[4]{n}$ is irrational.

(c) Give necessary and sufficient conditions on integers a and b so that the polynomial

$$h(x) = x^4 + ax^3 + bx - 1$$

has at least one rational root. □

Problem 8 (20 points). Recall a subset I is $\mathbb{Z}$ is an ***ideal*** if and only if it is closed under taking sums and if $a \in I$ and $n \in \mathbb{Z}$, then $na \in I$. We have shown if I is an ideal then for some integer $d \geq 0$ there holds $I = d\mathbb{Z} = \{nd : n \in \mathbb{Z}\}$. That is an ideal is just the set of all integral multiples of some $d \geq 0$.

Let a, b, c be integers not all zero and let

$$I = \{ax + by + cz : x, y, z \in Z\}$$

be the set of all integral linear combinations of a, b, and c.

(a) Prove that I is an ideal.

(b) Since I is an ideal and a, b, and c are not all zero, we have that $I = d\mathbb{Z}$ for some $d > 0$ (as $d = 0$ is ruled out as $a, b, c \in I$ and so I has a nonzero element). You can assume all of this. Use it to show that if k is an integer that divides all three of a, b, and c, then k also divides d. □

Problem 9 (10 points). Let a and b be positive integers with $\gcd(a, b) = 1$. Prove there are integers α and β such that

$$\alpha \equiv 1 \pmod a, \qquad \beta \equiv 0 \pmod a,$$
$$\alpha \equiv 0 \pmod b, \qquad \beta \equiv 1 \pmod b.$$

Hint: Start with the GCD is a linear combination theorem and if you look at that correctly you are 91% of the way done. □