Mathematics 546 Homework.

What are likely the most important result we have covered recently are

Theorem 1 (***GCD is linear combination***)**.** *Let a and b be integers, not both zero. Then there are integers x and y such that*

$$\gcd(a, b) = ax + by.$$

□

Recall that two integers a and b, not both zero, are ***relatively prime*** if and only if $\gcd(a, b) = 1$. That is if and only if the only integers that divide both a and b are ± 1.

Theorem 2. *Let a and b integers. Then a and b are relatively prime if and only if there are integers x and y such that*

$$ax + by = 1.$$

Problem 1. Prove this. *Hint:* If a and b are relatively prime, that is if $\gcd(a, b) = 1$, then that there are integers x and y with $ax + by = 1$ by Theorem 1. So you only have to prove that $ax+by = 1$ implies $\gcd(a, b) = 1$. To do this let $d = \gcd(a, b)$ use that d divides both a and b to show that d divides 1 □

Proposition 3. *Let $a, b, c \in \mathbb{Z}$ with $\gcd(a, b) = \gcd(a, c) = 1$. Then also $\gcd(a, bc) = 1$. (This is if a is relatively prime to each of b and c, then it is also relatively prime to the product bc.)*

Problem 2. Prove this. *Hint:* As has be said in class often the best way to use the hypothesis that two numbers are relatively prime is to use Theorem 2. Using this theorem we have integers x_1, y_1, x_2, y_2 with

$$\begin{aligned} ax_1 + by_1 &= 1 \\ cx_2 + dy_2 &= 1 \end{aligned}$$

Multiply these together:

$$(ax_1 + by_1)(cx_2 + dy_2) = 1^2 = 1$$

and show this can be rearranged in the form

$$aX + bcY = 1$$

for some integers X and Y. By Theorem 2 this shows that $\gcd(a, bc) = 1$. □

Proposition 4. *Let a and $b_1, b_2, \ldots, b_n$ in integers with $\gcd(a, b_j) = 1$ for $1 \le j \le n$. Then $\gcd(a, b_1 b_2 \cdots b_n) = 1$. (That is if a is relatively prime to each of a finite set of integers $b_1, b_2, \ldots, b_n$, then it is also relatively to the product $b_1 b_2 \cdots b_n$.)*

Problem 3. Prove this. *Hint:* This is really just a problem to let you practice using induction. □

Corollary 5. *If $\gcd(a, b) = 1$, then for any positive integer n*

$$\gcd(a, b^n) = 1.$$

Proof. In Proposition 4 let $b_1 = b_2 = \cdots = b_n = b$. $\square$

Problem 4. For the following pairs of numbers a and b use the Euclidean algorithm to find $\gcd(a,b)$ and find integers x and y with $ax+by = \gcd(a,b)$.

(a) $a = 135$, $b = 65$
(b) $a = 7684$, $b = 4148$.

Here you should review the Fundamental Theorem of Arithmetic as on page 20 of the text.

Recall that a number r is a ***rational number*** if and only if $r = a/b$ where a and b are integers. Here is an example of using the Fundamental Theorem of Arithmetic so show a number is irrational (that is it is not rational). Let

$$r = \frac{\ln 2}{\ln 3}.$$

We not show this is irrational. Assume, toward a contradiction, that it is rational. Then there are positive integers a and b such that

$$r = \frac{\ln 2}{\ln 3} = \frac{a}{b}.$$

Cross multiply to get

$$b \ln 2 = a \ln 3.$$

This can be rewritten as

$$\ln(2^b) = \ln(3^a),$$

which implies

$$2^b = 3^a.$$

But this is impossible as it would contradict the uniqueness part of the Fundamental Theorem of Arithmetic as the number $n = 2^b = 3^a$ would have two prime factorizations.

Problem 5. Show that the number

$$s = \frac{\ln 15}{\ln 14}$$

is irrational. $\square$

We are starting to study congruences. Our definition is

Definition 6. Let n be a positive integer and a and b any integers. Then a and b are ***congruent modulo*** n if and only if $n \mid (b-a)$. This is written as $a \equiv b \pmod{n}$. $\square$

Note this differs from the definition in the test (see page 28) where our definition is Proposition 1.3.2 on page 28. The most basic properties of congruence modulo n are given by

Theorem 7. *If n is a positive integer and a, b, c are any integers then congruence modulo n has the following properties*

(a) ***Reflexive property:*** $a \equiv a \pmod{n}$ *for all* $a \in \mathbb{Z}$

(b) ***Symmetric property:*** *$a \equiv b \pmod{n}$ implies $b \equiv a \pmod{n}$ for all $a, b \in \mathbb{Z}$*

(c) ***Transitive property:*** *$a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ implies $a \equiv c \pmod{n}$ for all $a, b, c \in \mathbb{Z}$.* □

Congruence is related to addition and multiplication as follows

Theorem 8. *If n is a positive integer and a, b, c, d are integers with*

$$a \equiv b \pmod{n} \qquad c \equiv d \pmod{n}$$

then

$$a + c \equiv b + d \pmod{n},$$
$$a - c \equiv b - d \pmod{n}$$

and

$$ac \equiv bd \pmod{n}.$$ □

Problem 6. Let n be a positive integer and $a, b, c, d \in \mathbb{Z}$. Let $x, y \in \mathbb{Z}$ with

$$x \equiv y \pmod{n}.$$

Prove that

$$ax^3 + bx^2 + cx + d \equiv ay^3 + by^2 + cy + d \pmod{n}.$$

□