Mathematics 300 Homework, November 4, 2017.

Recall that we have proven Bézout's Theorem: If a and b are positive integers, then there are integers x_0 and y_0 such that

$$ax_0 + by_0 = \gcd(a, b).$$

Definition. The integers a and b are ***relatively prime*** if $\gcd(a, b) = 1$. □

Then a special case of Bézout's Theorem is

Theorem 1. *Let a and b be relatively prime positive integers. Then there are integers x_0 and y_0 such that*

$$ax_0 + by_0 = 1.$$

In about 83.7% of the proofs where you are given that two numbers are relatively prime you will use Theorem 1.

The converse to Theorem 1 is also true.

Proposition 1. *Let a and b be integers and assume that there are integers x and y such with*

$$ax + by = 1.$$

Then a and b are relatively prime.

Problem 1. Prove this. *Hint:* Let $d = \gcd(a, b)$. We wish to show that $d = 1$. Use that $d \mid a$ and $d \mid b$ and the equation $ax + by = 1$ so show that $d \mid 1$. But the only positive divisor of 1 is 1. □

Here is an application of this.

Proposition 2. *If a and b are relatively prime, then so are a and b^2.*

Problem 2. Prove this. *Hint:* As a and b are relatively prime by Theorem 1 there are integers x_0 and y_0 such that

$$ax_0 + by_0 = 1.$$

Square this to get

$$a^2x_0^2 + 2ax_0by_0 + b^2y_0^2 = 1^2 = 1$$

Thus can be rewritten as

$$a(ax_0^2 + 2x_0by_0) + b^2(y_0)^2 = 1.$$

Now you should be able to use Proposition 1 to conclude that a and b^2 are relatively prime. □

The following is a fundamental result.

Theorem 2. *Let a and b be relatively prime positive integers and m any integer. If $a \mid bm$, then $a \mid m$.*

Problem 3. Prove this. *Hint:* Since a and b are relatively prime we start by using that there are integers x_0 and y_0 such that

$$ax_0 + by_0 = 1. \tag{*}$$

We are given that $a \mid bm$, therefore there is an integer q such that

$$bm = aq.$$

Multiply this equation by y_0 to get

$$by_0m = ay_0q. \tag{**}$$

Now solve for by_0 in equation (*)

$$by_0 = 1 - ax_0.$$

Use this formula for by_0 in equation (**) and rearrange to so that m can be written as $m = a(\text{stuff})$ and thus $a \mid m$. □

The following is the degree two case of what is often called the ***rational root test***.

Theorem 3. *Let a, b, c be integers with $a \neq 0$ and let*

$$r = \frac{p}{q}$$

be a rational root in lowest terms of the equation

$$ax^2 + bx + c = 0.$$

Then

$$p \mid c \qquad \text{and} \qquad q \mid a.$$

Proof that $p \mid c$. The assumption r is in lowest terms is just saying that $\gcd(p, q) = 1$. This time were are not going to use Theorem 1, but instead use Theorem 2. We are given that $r = p/q$ is a root of $ax^2 + bx + c = 0$. This means that

$$a\left(\frac{p}{q}\right)^2 + b\left(\frac{p}{q}\right) + c = 0.$$

Since fractions are a pain in the butt to deal with, we multiple by q^2 to clear of fractions. The result is

$$ap^2 + bpq + cq^2 = 0.$$

This can be rewritten as

$$cq^2 = -ap^2 - bpq = -p(ap + bq) = pk$$

where $k = -(ap + cq)$ is an integer. Therefore $p \mid cq^2$. We are assuming that $\gcd(p, q) = 1$. By Proposition 2 this implies that $\gcd(p, q^2) = 1$. That is p and q^2 are relatively prime.

So we now have $p \mid aq^2$ with p and q^2 relatively prime. By Theorem 2 this implies that $p \mid c$, which is just what we wanted to prove. □

Problem 4. With the set up of Theorem 3 prove that $q \mid a$. *Hint:* You should be able to modify the proof that $p \mid a$ cover this case. $\square$

Problem 5. Show that the equation

$$x^2 - 19 = 0$$

has no rational roots.

Solution: This is an equation of the form $ax^2 + bx + c = 0$ where $a = 1$, $b = 0$, and $c = -19$. This is all integers. So by Theorem 3 the only possible rational roots of this equation are of the form $r = p/q$ where $p \mid (-19)$ and $q \mid 1$. Thus the only possible choices for p and q are

$$p = \pm 1,\ \pm 19, \qquad \text{and} \qquad q = \pm 1.$$

Whence the only possible choices for a rational root r are

$$r = \frac{p}{q} = \pm 1, \pm 19.$$

Now we just check that none of these are roots.

$$(\pm 1)^2 - 19 = -18 \neq 0$$
$$(\pm 19)^2 - 19 = 342 \neq 0.$$

Since these are the only possible ration roots and none of them are roots, the equation has no rational roots. $\square$

Problem 6. Show that $\sqrt{19}$ is irrational.

Solution: The number $\sqrt{19}$ is a root of the equation $x^2 - 19 = 0$. But we saw in the last problem that this equation has no rational roots. Thus $\sqrt{19}$ must be irrational. $\square$

Problem 7. Show that $x^2 - 13$ has no rational roots. $\square$

Problem 8. Use the last problem to show that $\sqrt{13}$ is irrational. $\square$