MATH 315; HOMEWORK # 1

Due Jan 19, 2015

1. (page 11, Exercise 1.3) The consecutive odd numbers 3,5, and 7 are all primes. Are there infinitely many such "prime triplets"? That is, are there infinitely many prime numbers p so that $p+2$ and $p+4$ are also primes? [Hint: Divide into two cases; $p \equiv 1 \pmod 3$ and $p \equiv 2 \pmod 3$.]

2. (page 23, Exercise 3.2) (a) Use the lines through the point (1,1) to describe all of the points on the circle $x^2+y^2=2$ whose coordinates are rational numbers.

(b) What goes wrong if you try to apply the same procedure to find all of the points on the circle $x^2+y^2=3$ with rational coordinates? (Hint: there are no rational points on the circle; if $x=\frac{a}{b}, y=\frac{c}{d}$, where $gcd(a,b)=1, gcd(c,d)=1$, then $(ad)^2+(bc)^2=3(bd)^2$. Show that there are no integer solutions for $u^2+v^2=3w^2$, by considering the remainder of both sides when divided by 4.)

3. (page 23, Exercise 3.3) Find a formula for all of the points on the hyperbola $x^2-y^2=1$ whose coordinates are rational numbers. [Hint. Take the line through the point (-1,0) having rational slope m and find a formula in terms of m for the second point where the line intersects the hyperbola.]

4.(page 23, Exercise 3.4) The curve $y^2=x^3+8$ contains the points (1,-3) and $(-\frac{7}{4},\frac{13}{8})$. The line through these two points intersects the curve in exactly one other point. Find this third point. Can you explain why the coordinates of this third point are rational numbers?

5. (page 35, Exercise 5.3) Let $b=r_0, r_1, r_2, ...$ be the successive remainder in the Euclidean algorithm applied to a and b. Show that every two steps reduces the remainder by at least one half. In other words, verify that $r_{i+2} < \frac{1}{2} r_i$ for every $i=0,1,2,...$ Conclude that the Euclidean algorithm will terminate in at most $2\log_2(b)$ steps, where $\log_2$ is the logarithm to the base 2. In particular, show that the number of steps is at most seven times the number of digits in b. [Hint. What is the value of $\log_2(10)$?]

6. (page 35, Exercise 5.4) A number L is called a common multiple of m and n if both m and n divide L. The smallest such L is called the least common multiple of m and n and is denoted by $LCM(m,n)$. For example, $LCM(3,7)=21$ and $LCM(12,66)=132$.

(1) Find the following least common multiples: (i) $LCM(8,12)$ (iii) $LCM(51,68)$
(2) For each of the LCMs you computed in (1), compare the value of $LCM(m,n)$ to the values of m, n, and $gcd(m,n)$. Try to find a relationship.
(3) Give an argument proving that the relationship you found is correct for all m and n.
(4) Use your result in (2) to compute $LCM(301337, 307829)$.
(5) Suppose that $gcd(m,n)=18$ and $LCM(m,n)=720$. Find m and n. Is there more than one possibility. If so, find all of them.