MATH 412 HW 2: September 10, 2015

BILLY BOB

***1.** Let a and $b \in \mathbb{Z}$ with $b > 0$. If

$$a = bq + r, \quad 0 \leq r < b,$$

then $\gcd(a, b) = \gcd(b, r)$.

Solution:

2. **a.** Show that if a and b are integers satisfying $a^2 = 2b^2$ then $a = b = 0$. **Hint:** Use the Fundamental Theorem of Arithmetic.

Solution:

b. Show that $\sqrt{2}$ is irrational.

Solution:

3. Let p and q be primes such that $p \geq 5$ and $q \geq 5$. Show that

$$24 \mid (p^2 - q^2).$$

This problem is a bit hard. If you can't do it, try to show that $12 \mid (p^2 - q^2)$ and I'll give you partial credit.

Solution:

Note $p^2 - q^2 = (p+q)(p-q)$. First we show that $8 \mid p^2 - q^2$. Since p and q are both prines greater than or equal to 5, they are odd. So $p + q$ and $p - q$ are both even. Since the product of two even numbers is divisible by 4, we see that $4 \mid p^2 - q^2$. If $4 \mid p + q$ or $4 \mid p - q$ then 8 divides their product. Suppose that both $p + q$ and $p - q$ are congruenct to $2 \pmod 4$. Then

$$\begin{aligned} p + q &= 4k + 2 \\ p - q &= 4t + 2. \end{aligned}$$

Adding these equations gives $2p = 4(k + t) + 4 = 4(k + t + 1)$. Dividing both sides by 2 gives $p = 2(k + t + 1)$, proving p is even. This is a contradiction. So 4 divides either $p + q$ or $p - q$ (and the other one is even). So $8 \mid p^2 - q^2$.

Now we show that $3 \mid p^2 - q^2$. Since both p and q are greater than or equal to 5, neither is divisible by 3. Let

$$p \equiv a \pmod 3, \quad a = 1 \text{ or } 2$$
$$q \equiv b \pmod 3, \quad b = 1 \text{ or } 2$$

If $a = b$ the $p - q \equiv 0 \pmod 3$. If a and b are different, then their sum is 3 and $p+q \equiv 0 \pmod 3$ in this case. Thus $3 \mid p-q$ or $3 \mid p+q$, and so $3 \mid p^2 - q^2$.

Finally since $\gcd(3,8) = 1$, we conclude $3 \cdot 8 = 24 \mid p^2 - q^2$, as the student can show. (Note $6 \mid 12$ and $4 \mid 12$ but $24 = 6 \cdot 4 \nmid 12$, so we needed $\gcd(3,8) = 1$ to conclude $24 \mid p^2 - q^2$.)