MA 630 - Homework 5 (Module 3 - Section 1)

Solutions must be typeset in LaTeX and submitted to Canvas as a .pdf file. When applicable, write in complete sentences. Use only results which have been discussed in our class.

1. Let $n \in \mathbb{Z}$. Prove that $\gcd(5n+2, 12n+5) = 1$.

   Since we have that $(-12)(5n+2) + (5)(12n+5) = 1$ then setting $a = 5n+12$ and $b = 12n+5$ we have that

   $$1 \in \{ax + by | x, y \in \mathbb{Z}\}.$$

   There is no natural number less than 1, so 1 is the least such natural number. Hence by theorem 3.10 we have that $\gcd(a,b) = 1$. □

2. Let a and b be integers which are not both zero, and let $d = \gcd(a,b)$. Prove that $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

   Proof: By Theorem 3.10 we know there are $m, n \in \mathbb{Z}$ such that $am + bn = d$. Hence $\left(\frac{a}{d}\right) m + \left(\frac{b}{d}\right) n = 1$ and therefore

   $$1 \in \left\{ \left(\frac{a}{d}\right) m + \left(\frac{b}{d}\right) n | m, n \in \mathbb{Z} \right\}.$$

   Since there is no natural number less than 1, then 1 is the least natural number in the set. We also know that $\frac{a}{d}$ is a natural number since d divides a and therefore $a = dp$ for some natural number p. Hence $\frac{a}{d} = p$ which is a natural number. By the same argument, $\frac{b}{d}$ is a natural number. Hence by theorem 3.10 it follows that $gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$. □

3. Let $a, b, q, r \in \mathbb{Z}$ with $b \neq 0$. Prove that if $a = bq + r$, then $\gcd(a,b) = \gcd(b,r)$. *Hint: Let* $d = \gcd(a,b)$. *Use Theorem 3.9 to characterize* $\gcd(b,r)$, *and then show that* $d = \gcd(b,r)$.

   Proof: Suppose $a = bq + r$ with $b \neq 0$. By definition $\gcd(b,r)$ divides both b and r. So let m, n be integers such that $b = m\gcd(b,r)$ and $r = n\gcd(b,r)$. Then since

$$a = m\gcd(b,r)q + n\gcd(b,r) = \gcd(b,r)(mq+n)$$

we now have that $\gcd(b,r)$ divides a. Since we have already noted that $\gcd(b,r)$ divides b, then $\gcd(b,r)$ satisfies the first property of theorem 3.9 applied to $d = gcd(a,b)$.

Next let c be any integer which divides a and b. Let $a = cf$ and $b = cg$. We want to show that c divides $\gcd(b,r)$, in order to demonstrate the second property of 3.9. Now by theorem 3.10 we have that $\gcd(b,r) = bx + ry$ for some integers x, y. Moreover, since $r = a - bq$ then

$$\gcd(b,r) = cgx + (a - bq)y = cgx + cf - cgqy = c(gx + f - gqy).$$

This shows that c divides $\gcd(b,r)$ as desired.

Hence by theorem 3.9 $\gcd(b,r) = \gcd(a,b)$.

4. Use the Euclidean algorithm to find an integer x such that $2314x - 1$ is divisible by 3181.

   We apply the Euclidean algorithm to 2314 and 3181:

$$\begin{aligned} 3181 &= 2314 \cdot 1 + 867 & \qquad 867 &= 3181 - 2314 \\ 2314 &= 867 \cdot 2 + 580 & 580 &= 2314 - 867 \cdot 2 \\ 867 &= 580 \cdot 1 + 287 & 287 &= 867 - 580 \\ 580 &= 287 \cdot 2 + 6 & 6 &= 580 - 287 \cdot 2 \\ 287 &= 6 \cdot 47 + 5 & 5 &= 287 - 6 \cdot 47 \\ 6 &= 5 \cdot 1 + 1 & 1 &= 6 - 5 \\ 5 &= 1 \cdot 5 + 0. \end{aligned}$$

$$
\begin{aligned}
1 &= 6 - 5 \\
&= 6 - (287 - 6 \cdot 47) \\
&= 6 \cdot 48 - 287 \\
&= (580 - 287 \cdot 2) \cdot 48 - 287 \\
&= 287 \cdot (-97) + 580 \cdot 48 \\
&= (867 - 580) \cdot (-97) + 580 \cdot 48 \\
&= 580 \cdot (145) - 867 \cdot 97 \\
&= (2314 - 867 \cdot 2) \cdot 145 - 867 \cdot 97 \\
&= -867 \cdot 387 + 2314 \cdot 145 \\
&= -(3181 - 2314) \cdot 387 + 2314 \cdot 145 \\
&= 2314 \cdot 532 - 3181 \cdot 387.
\end{aligned}
$$

This then shows that

$$3181 \cdot 387 = 2314 \cdot 532 - 1$$

which shows that 3181 divides $2314 \cdot 532 - 1$, and so a choice for x is 532.

5. Let $p \geq 5$ be a prime.

   (a) Use the division algorithm to prove that there exists $k \in \mathbb{Z}$ such that either $p = 6k + 1$ or $p = 6k - 1$.

   (b) Prove that 24 divides $p^2 - 1$. *Hint: The integer k in part (a) is either even or odd.*

(a) Proof: By the division algorithm there must exist some q_1 and $0 \leq r_1 < 3$ such that $p = 3q_1 + r_1$. Also there must exist some q_2 and $0 \leq r_2 < 2$ such that $p = 2q_2 + r_2$. Also $r_1 \neq 0$ otherwise we have that 3 divides p, which cannot be true since p is prime and greater than 4. Similarly $r_2 \neq 0$, and in this case the only possibility then is $r_2 = 1$. Hence $p = 2q_2 + 1$.

The remaining cases for r_1 are $r_1 = 1, 2$. If $r_1 = 1$ then

$$p = 3q_1 + 1 = 2q_2 + 1$$

and so $3q_1 = 2q_2$. Since 3 is prime, and 3 does not divide 2, then by corollary 3.13 we have that 3 divides q_2, so write $q_2 = 3k$. Then we have

$$p = 2q_2 + 1 = 2(3k) + 1 = 6k + 1$$

On the other hand if $r_1 = 2$ then

$$p = 3q_1 + 2 = 2q_2 + 1$$

so $3q_1 + 1 = 2q_2$. Since $2q_2$ is even, the quantity on the left must be as well. But then 1 is odd, and an odd plus an even is odd. So $3q_1$ cannot be even, and must be odd. If q_1 were even then $3q_1$ would be even, so we must have q_1 is odd. (Note: I'm hoping at this point in the course we can freely use facts like these.) So let $q_1 = 2m + 1$ for some integer m. Therefore

$$\begin{aligned} p &= 3q_1 + 2 \\ &= 3(2m+1) + 2 \\ &= 6m + 5 \\ &= 6(m+1) - 6 + 5 \\ &= 6(m+1) - 1. \end{aligned}$$

Setting $k = m + 1$ we then have that $p = 6k - 1$.

In both cases we have seen that either $p = 6k + 1$ or $p = 6k - 1$. Since this exhausts all possible cases, the proof is complete. $\square$

(b) Proof: We have that

$$p^2 - 1 = (p+1)(p-1).$$

If $p = 6k + 1$ then

$$\begin{aligned}(p+1)(p-1) &= (6k+2)(6k)\\ &= 12k(3k+1).\end{aligned}$$

In that case, either k is even or odd. If k is even and $k = 2m$ then

$$\begin{aligned}(p+1)(p-1) &= 12(2m)(3k+2)\\ &= 24m(3k+2)\end{aligned}$$

which shows that $p^2 - 1$ is divisible by 24. On the other hand if k is odd then let $k = 2m + 1$. Therefore

$$\begin{aligned}(p+1)(p-1) &= 12k(3(2m+1)+1)\\ &= 12k(6m+4)\\ &= 24k(3m+2)\end{aligned}$$

which again shows that $p^2 - 1$ is divisible by 24.

Now we consider the case where $p = 6k - 1$. Then

$$\begin{aligned}p^2 - 1 &= (p+1)(p-1)\\ &= 6k(6k-2)\\ &= 12k(3k-1).\end{aligned}$$

Now if k is even and $k = 2m$ then

$$p^2 - 1 = 24m(3k-1)$$

and we have $p^2 - 1$ is divisible by 24. If k is odd and $k = 2m + 1$ then

$$
\begin{aligned}
p^2 - 1 &= 12k(3(2m+1) - 1) \\
&= 12k(6m+2) \\
&= 24k(3m+1).
\end{aligned}
$$

Again this shows $p^2 - 1$ is divisible by 24. Since this exhausts all possible cases, then we must have that $p^2 - 1$ is divisible by 24. $\square$