Math 333 Problem Set 3
Due: 02/24/16
Solutions

1. Use the Euclidean algorithm to find $\gcd(5858, 1436)$. Write $\gcd(5858, 1436)$ as a linear combination of 5858 and 1436.

We have

$$\begin{aligned}
5858 &= 1436(4) + 114 \\
1436 &= 114(12) + 68 \\
114 &= 68(1) + 46 \\
68 &= 46(1) + 22 \\
46 &= 2(22) + 2 \\
22 &= 2(11).
\end{aligned}$$

Thus, we have $\gcd(5858, 1436) = 2$. To write 2 as a linear combination of 5858 and 1436 we use these equations. First, note

$$\begin{aligned}
2 &= 46 + 22(-2) \\
22 &= 68 + 46(-1) \\
46 &= 114 + 68(-1) \\
68 &= 1436 + 114(-12) \\
114 &= 5858 + 1436(-4).
\end{aligned}$$

Thus, we have

$$\begin{aligned}
2 &= 46 + 22(-2) \\
&= 46 + (-2)(68 + 46(-1)) \\
&= 68(-2) + 46(3) \\
&= 68(-2) + 3(114 + 68(-1)) \\
&= 114(3) + 68(-5) \\
&= 114(3) + (-5)(1436 + 114(-2)) \\
&= 1436(-5) + 114(63) \\
&= 1436(-5) + 63(5858 + 1436(-4)) \\
&= 5858(63) + 1436(-257).
\end{aligned}$$

2. Prove that if $\gcd(a,b) = d$ then $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

   Proof. Let $d = \gcd(a,b)$. There exists $m, n \in \mathbb{Z}$ so that $d = am + bn$. Since $d \mid a$ there exists $s \in \mathbb{Z}$ so that $a = ds$ and since $d \mid b$ there exists $t \in \mathbb{Z}$ so that $b = dt$. We have

   $$\begin{aligned} d &= am + bn \\ &= dsm + dtn \\ &= d(sm + tn), \end{aligned}$$

   i.e., $1 = sm + tn$. From our result in class this gives $\gcd(s,t) = 1$, i.e., $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$. □

3. Prove that $\gcd(a,b) = \gcd(a, b + at)$ for all $t \in \mathbb{Z}$.

   Proof. Let $d = \gcd(a,b)$ and $e = \gcd(a, b + at)$. Note that since $d \mid a$ and $d \mid (b + at)$, we must have $d \mid e$. Similarly, we have $e \mid a$ and $e \mid b = (b + at) - a(t)$. Thus $e \mid d$. Since d, e are both positive integers and they divide each other, they must be equal. □

4. Prove or disprove: If p is a prime and $p \mid (a^2 + b^2)$ and $p \mid (c^2 + d^2)$, then $p \mid (a^2 - c^2)$.

   Let $p = 2$. Then $p \mid (2^2 + 0^2) = 4$ and $p \mid (1^2 + 1^2) = 2$, but $p \nmid (2^2 - 1^2) = 3$.

5. Prove that if $c^2 = ab$ and $\gcd(a,b) = 1$ then a and b are perfect squares.

   Proof. Let p be a prime that divides a. Then $p \mid c^2 = c \cdot c$, so $p \mid c$. Write $c = p^m d$ for $m, d \in \mathbb{Z}_{\geq 1}$ where $p \nmid d$. Then we have $c^2 = p^{2m} d^2$. Since $\gcd(a,b) = 1$, we must have that $p \nmid b$, i.e., $\gcd(p^{2m}, b) = 1$. Since $p^{2m} \mid ab$ and $\gcd(p^{2m}, b) = 1$, we must have $p^{2m} \mid a$. Moreover, we cannot have $p^{2m+1} \mid a$ as this would imply $p^{2m+1} \mid c^2$. Thus, $a = p^{2m} e$ for some $e \in \mathbb{Z}_{\geq 1}$ with $p \nmid e$. This shows that every prime that divides a occurs to an even power in the prime factorization of a, i.e., a is a perfect square. The same argument works to show b is a perfect square. □

6. Recall that one has $(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k}$ where $\binom{p}{k} = \frac{p!}{k!(p-k)!}$. Prove that if p is prime and $0 < k < p$ then $p \mid \binom{p}{k}$.

Proof. Let $0 < k < p$. We have $\binom{p}{k} \in \mathbb{Z}$. Thus, $k!(p-k)! \mid p!$. Observe that since $0 < k < p$ we have $p \nmid k!$ and $p \nmid (p-k)!$. Since p is prime, we must have $\gcd(p, k!) = 1 = \gcd(p, (p-k)!)$. Thus, it must be the case that $k!(p-k)! \mid (p-1)!$, i.e., $\frac{(p-1)!}{k!(p-k)!} \in \mathbb{Z}$, so $p \mid \binom{p}{k}$ as desired. □

7. If $r \equiv 3 \pmod{10}$ and $s \equiv -7 \pmod{10}$, what is $2r + 3s$ congruent to modulo 10?

We have

$$\begin{aligned} 2r + 3s &\equiv 2(3) + 3(-7) \pmod{10} \\ &\equiv -15 \pmod{10} \\ &\equiv 5 \pmod{10}. \end{aligned}$$

8. If $a \equiv b \pmod{n}$ and $k \mid n$, is it true that $a \equiv b \pmod{k}$? If so, prove it. If not, give a counterexample.

Proof. Since $k \mid n$ there exists $m \in \mathbb{Z}$ so that $n = mk$. The fact that $a \equiv b \pmod{n}$ means $n \mid (a - b)$, i.e., there exists $d \in \mathbb{Z}$ so that $a - b = nd = (mk)d$. Thus, $k \mid (a - b)$, i.e., $a \equiv b \pmod{k}$. □