Math347, Spring 2018, Homework #10, Solution
Due Wednesday, April 18, 2018

Page 134, 6.18. Suppose $\gcd(a, b) = 1$,

1) Does this determine $\gcd(a^2, b^2)$? Explain your answer.
Answer: Yes. If $\gcd(a, b) = 1$, then $\gcd(a^2, b^2) = 1$.

Proof: Suppose $\gcd(a^2, b^2)$ has a prime factor $p > 1$. Then we have $p|a^2$ and $p|b^2$ and thus we must have $p|a$ and $p|b$. Therefore, $p|\gcd(a, b)$, but by assumption $\gcd(a, b) = 1$. Contradiction. So we must have $gcd(a^2, b^2) = 1$.

Another Proof: We can look at the prime factorizations of

$$a = p_1^{n_1} \cdots p_k^{n_k} \text{ and } b = q_1^{m_1} \cdots q_l^{m_l}.$$

If $\gcd(a, b) = 1$, then $p_1, \cdots, p_k$ are all distinct from $q_1, \cdots, q_l$. It is easy to see that

$$a^2 = p_1^{2n_1} \cdots p_k^{2n_k} \text{ and } b^2 = q_1^{2m_1} \cdots q_l^{2m_l}$$

have distinct prime factors. This shows $\gcd(a^2, b^2) = 1$.

2) Does this determine $\gcd(a, 2b)$?

Answer: This will depend on whether a is an odd number, or an even number. Considering the prime factorizations of a and b, it is easy to see that

If a is odd, then all prime factors of a are distinct from 2 and distinct from the prime factors of b. Then $\gcd(a, 2b) = 1$.

If a is even, then b must be odd and thus $\gcd(a, 2b) = 2$.

Page 134, 28. Suppose that $\gcd(a, b) = 1$ and that $a|n$ and $b|n$. Prove that $ab|n$.

Proof: Since $\gcd(a, b) = 1$, we get $1 = sa + tb$ for some $s, t \in \mathbb{Z}$.
Since $a|n$ and $b|n$, we can write $n = xa$ and $n = yb$ for some $x, y \in \mathbb{Z}$. It follows that

$$n = sna + tnb = syba + txab = (sy + tx)ab.$$

Therefore, $ab|n$.

Page 134, 6.37 a). Let p be a prime number. Prove that p divides $\binom{p}{k}$ if $1 \leq k \leq p-1$.
Proof: We first note that since $1 \leq k \leq p-1$, p must be relatively prime with $2, 3, \cdots, k$. It follows that $\gcd(p, k!) = 1$. Similarly, since $1 \leq p-k \leq p-1$, we must have $\gcd(p, (p-k)!) = 1$.

Since $\binom{p}{k} = \frac{p!}{k!(p-k)!}$, we get

$$k!(p-k)!\binom{p}{k} = p! = p(p-1)\cdots 1.$$

This shows that p divides $k!(p-k)!\binom{p}{k}$, and thus p divides $\binom{p}{k}$ (according to a theorem we proved in class).

Page 151, 7.1. Let a, b, x, n be positive integers. The following statement is not always true: If $ax \equiv bx \bmod n$, then $a \equiv b \bmod n$. Provide a counterexample, and add a hypothesis on x and n to make the statement true.

Counterexample: We can consider $n = 4$, $x = 2$, $a = 2$, and $b = 0$. Then it is clear that $2 \cdot 2 \equiv 0 \cdot 2 \equiv 0 \bmod 4$. But 2 is not congruent to 0 mod 4.

Additional hypothesis: If $\gcd(x, n) = 1$, then we must have $a \equiv b \bmod n$.
Proof: If there exists x such that $ax \equiv bx \bmod n$, then we have

$$(a-b)x = ax - bx = kn$$

for some $k \in \mathbb{Z}$. From this, we see that $n|(a-b)x$. Since $gcd(x, n) = 1$, relatively prime, we must have $n|a-b$. This shows that $a \equiv b \bmod n$.

Additional Problem: Prove that $5^{\frac{1}{3}}$ is an irrational number.
Proof: Suppose that $5^{\frac{1}{3}}$ is rational. Then there exist positive integers r and s such that $\gcd(r, s) = 1$ and $5^{\frac{1}{3}} = \frac{r}{s}$. We claim that $s = 1$.

Suppose $s \neq 1$. Then $s \geq 2$ and there exists a prime number $p|s$. Since

$$5 = \frac{r^3}{s^3} \text{ or equivalently, } s^3 5 = r^3,$$

we see that $p|s^3 5 = r^3$ and thus $p|r$. This shows that $p \geq 2$ is a common divisor of s and r, which contradicts to the fact that $\gcd(r, s) = 1$. Therefore, we must have $s = 1$ and thus $5^{\frac{1}{3}} = r$ is a positive integer. This is impossible since $5 \neq r^3$ for any positive integer $r \in \mathbb{N}$. Therefore, $5^{\frac{1}{3}}$ must be an irrational number.