Math 446 - Homework # 3

1. *Prove the following:*

   (a) *Given $a, b \in \mathbb{Z}$ with $b \neq 0$, there exist $x, y \in \mathbb{Z}$ with $\gcd(x, y) = 1$ and $\frac{a}{b} = \frac{x}{y}$.*

   Solution: Let $d = \gcd(a, b)$. Let $x = a/d$ and $y = b/d$. Then from class, we know that $\gcd(x, y) = 1$. And we also have that $a/b = (a/d)/(b/d) = x/y$.

   (b) *If p is a prime and a is a positive integer and $p|a^n$, then $p^n|a^n$.*

   Solution: Suppose that p is a prime and p divides $a^n = a \cdot a \cdots a$. Recall that when a prime divides a product of integers then it must divide at least one of the integers contained in the product. Hence $p|a$. Therefore, $pk = a$ for some integer k. Hence, $a^n = (pk)^n = p^n k^n$. Therefore $p^n|a^n$.

   (c) *$\sqrt[5]{5}$ is irrational.*

   Solution: Suppose that $\sqrt[5]{5}$ is rational. Then $\sqrt[5]{5} = a/b$ where $a, b \in \mathbb{Z}$. We may always cancel common divisors in a fraction, hence we may assume that $\gcd(a, b) = 1$.

   Taking the fifth power of both sides of $\sqrt[5]{5} = a/b$ gives $5 = a^5/b^5$. Hence $a^5 = 5b^5$. Therefore 5 divides the product $a^5 = a \cdot a \cdot a \cdot a \cdot a$. Recall that when a prime divides a product of integers then it must divide at least one of the integers contained in the product. Since 5 is prime we must have that 5 divides a. Therefore $a = 5k$ where k is an integer. Substituting this expression into $a^5 = 5b^5$ yields $5^5k^5 = 5b^5$. Hence $5(5^3k^5) = b^5$. Therefore 5 divides b^5. Since 5 is prime we must have that $5|b$. But then 5 would be a common divisor of a and b and hence $\gcd(a, b) \geq 5$. This contradicts our assumption that $\gcd(a, b) = 1$.

   Therefore $\sqrt[5]{5}$ is irrational.

   (d) *If p is a prime, then $\sqrt{p}$ is irrational.*

   Solution: Suppose that $\sqrt{p}$ is rational. Then $\sqrt{p} = a/b$ where $a, b \in \mathbb{Z}$. We may always cancel common divisors in a fraction, hence we may assume that $\gcd(a, b) = 1$.

   Squaring both sides of $\sqrt{p} = a/b$ and then multiplying through by b^2 gives us that $pb^2 = a^2$. Hence $p|a^2$. Recall that when a prime divides a product of integers then it must divide at least one of the integers in the product. Since p is a prime, p must divide a. Therefore, $a = pk$ for some integer k. Substituting this back into $pb^2 = a^2$ gives us that $pb^2 = p^2k^2$. Dividing by p gives us $b^2 = pk^2$. Thus $p|b^2$. Again, since p is a prime, we must have that $p|b$.

From the above arguments we see that $p|a$ and $p|b$. Hence $\gcd(a, b) \geq p$. However, we also have that $\gcd(a, b) = 1$. This gives us a contradiction.

2. (a) *Suppose that a, b, c are integers with $a \neq 0$ and $b \neq 0$. If $a|c$, $b|c$, and $\gcd(a, b) = 1$, then $ab|c$.*

    Solution 1: Since $a|c$ and $b|c$ we have that $c = at$ and $c = br$ where $r, t \in \mathbb{Z}$. Therefore $at = br$. Thus $a|br$. Since $\gcd(a, b) = 1$ and $a|br$ we have that $a|r$. Thus $r = ak$ where $k \in \mathbb{Z}$. Thus, $c = br = bak = (ab)k$. Hence $ab|c$.

    Solution 2: Since $a|c$ and $b|c$ we have that $c = at$ and $c = br$ where $r, t \in \mathbb{Z}$. Since $\gcd(a, b) = 1$, there exist integers x and y with $ax + by = 1$. Multiplying this by c we get that $acx + bcy = c$. Now substitute $c = br$ into the first term and $c = at$ into the second term to get that $c = acx + bcy = abrx + baty = (ab)(rx + ty)$. Therefore $ab|c$.

   (b) *Prove that $\sqrt{6}$ is irrational.*

    Solution: Suppose that $\sqrt{6}$ was rational. We show that this leads to a contradiction. We may write $\sqrt{6} = x/y$ where x and y are integers with $y \neq 0$ and $\gcd(x, y) = 1$. Squaring this equation and cross-multiplying we get that $6y^2 = x^2$ or $2 \cdot 3 \cdot y^2 = x^2$. Therefore, 2 divides $x^2 = x \cdot x$. Since 2 is prime we must have that 2 divides x. Similarly, 3 divides $x^2 = x \cdot x$. And since 3 is prime we must have that 3 divides x. Since $2|x$ and $3|x$ and $\gcd(2, 3) = 1$, by the first part of this problem, we have that $6 = 2 \cdot 3$ must divide x. So $x = 6u$ where u is a non-zero integer. Subbing this into $6y^2 = x^2$ gives us that $6y^2 = 6^2u^2$. Thus $y^2 = 6u^2$. Following the same reasoning as above, this forces that 6 must divide y. Therefore, 6 is a common divisor of x and y which contradicts the fact that $\gcd(x, y) = 1$.

3. *Prove that $\log_{10}(2)$ is an irrational number.*

Solution: Suppose that $\log_{10}(2)$ was rational. Then $\log_{10}(2) = a/b$ where a and b are positive integers (we may assume they are positive since $\log_{10}(2)$ is positive). In particular, $b \neq 0$. We have that $10^{a/b} = 2$ by the definition of the logarithm. Hence $10^a = 2^b$. Therefore $2^a 5^a = 2^b$. Since prime factorizations are unique (by the fundamental theorem of arithmetic) we must have that $a = 0$ since there are no factors of 5 on the right-hand side of $2^a 5^a = 2^b$. Hence $2^0 5^0 = 2^b$. This gives $2^b = 1$. But this implies that $b = 0$ which is not true. Hence $\log_{10}(2)$ is irrational.

4. *We say that an integer $n \geq 2$ is a* **perfect square** *if $n = m^2$ for some integer $m \geq 2$. Prove that n is a perfect square if and only if the prime factorization of $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ has even exponents (that is, all the k_i are even).*

   Solution: Suppose that n is a perfect square. Therefore $n = m^2$ where m is a positive integer. By the fundamental theorem of arithmetic $m = q_1^{e_1} q_2^{e_2} \cdots q_r^{e_r}$ where q_i are primes and e_j are positive integers. We see that

   $$n = m^2 = (q_1^{e_1} q_2^{e_2} \cdots q_r^{e_r})^2 = q_1^{2e_1} q_2^{2e_2} \cdots q_r^{2e_r}.$$

   Therefore every prime in the prime factorization of n is raised to an even exponent.

   Conversely suppose that every prime in the prime factorization of n is raised to an even exponent. Then $n = p_1^{2k_1} p_2^{2k_2} \cdots p_r^{2k_r}$ where p_i are primes and k_j are positive integers. Let $m = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$. Then m is an integer and $n = m^2$. Hence n is a perfect square.

5. (a) *Let a and b be positive integers. Prove that $\gcd(a, b) > 1$ if and only if there is a prime p satisfying $p|a$ and $p|b$.*

   Solution:

   Suppose that $d = \gcd(a, b) > 1$. Since d is positive integer with $d \geq 2$, by the fundamental theorem of arithmetic, there is at least one prime p with $p|d$. Since $p|d$ and $d|a$ we must have that $p|a$. Since $p|d$ and $d|b$ we must have that $p|b$. Hence $p|a$ and $p|b$.

   Conversely suppose that there is a prime p with $p|a$ and $p|b$. Then $\gcd(a, b) \geq p > 1$.

(b) *Let a, b, and n be positive integers. Prove that if* $\gcd(a,b) > 1$ *if and only if* $\gcd(a^n, b^n) > 1$.

Solution: Suppose that $d = \gcd(a,b) > 1$. So $a = dk$ and $b = dm$ where k and m are integers. Thus $a^n = d^n k^n$ and $b^n = d^n m^n$. So $d|a^n$ and $d|b^n$. Hence $\gcd(a^n, b^n) \geq d > 1$.

Conversely, suppose that $\gcd(a^n, b^n) > 1$. Then by exercise (5a), there exists a prime q with $q|a^n$ and $q|b^n$. Since q divides the product $a^n = a \cdot a \cdots a$ and q is prime, we must have that $q|a$. Since q divides the product $b^n = b \cdot b \cdots b$ and q is prime, we must have that $q|b$. Hence $q|a$ and $q|b$. Thus $\gcd(a,b) \geq q > 1$.

6. *Suppose that x and y are positive integers where $4|xy$ but $4 \nmid x$. Prove that $2|y$.*

Solution: Since $4|xy$ we have that $4s = xy$ for some integer s. Hence $2(2s) = xy$. Thus $2|xy$. Since 2 is prime we have that either $2|x$ or $2|y$. We break this into cases.

case 1: If $2|y$ then we are done.

case 2: Suppose that $2|x$. Then $x = 2k$ where k is some integer. Since $4 \nmid x$ we must have that k is odd. Hence $2 \nmid k$. Substituting $x = 2k$ into $4s = xy$ gives $4s = 2ky$. Hence $2s = ky$. Therefore $2|ky$. Since 2 is prime we must have either $2|k$ or $2|y$. But $2 \nmid k$. Therefore, $2|y$.

7. *Let a and b be positive integers. Suppose that 5 occurs in the prime factorization of a exactly four times and 5 occurs in the prime factorization of b exactly two times. How many times does 5 occur in the prime factorization of $a + b$?*

Solution: By assumption $a = 5^4 s$ and $b = 5^2 t$ where s and t are positive integers and $5 \nmid s$ and $5 \nmid t$. Note that $a + b = 5^2(25s + t)$. We want to show that 5 does not divide $25s+t$. If 5 did divide $25s+t$ then $5k = 25s + t$ for some integer k. This would imply that $5(k - 5s) = t$, which gives that 5 divides t. But we know that is not true.

Therefore $a + b = 5^2(25s + t)$ where 5 does not divide $25s + t$. Hence 5 occurs twice in the prime factorization of $a + b$.

8. *A positive integer $n \geq 2$ is called* **squarefree** *if it is not divisible by any perfect square. For example, 12 is not squarefree because $4 = 2^2$*

is a perfect square and $4|12$. *However,* 10 *is squarefree. (Recall the definition of perfect square from problem 4.*

(a) *Prove that a positive integer* $n \geq 2$ *is squarefree if and only if* n *can be written as the product of distinct primes.*

Solution: Suppose that n is squarefree. Let $n = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}$ be the prime factorization of n where the p_i are distinct. Here we have that the e_i are positive integers. Suppose that $e_1 \geq 2$. Then $n = p_1^2(p_1^{e_1-2} p_2^{e_2} \cdots p_s^{e_s})$. This would imply that n was divisible by the perfect square p_1^2. This can't happen since n is squarefree. Hence $e_1 = 1$. A similar argument shows that $e_i = 1$ for all i. Thus $n = p_1 p_2 \cdots p_s$ is the product of distinct primes.

Conversely suppose that n is the product of distinct primes. By way of contradiction, suppose that n was divisible by a perfect square. Then $n = m^2 k$ where $m \geq 2$ and $k \geq 1$ are integers. Let $m = q_1^{f_1} q_2^{f_2} \cdots q_t^{f_t}$ be the prime factorization of m where the q_i are primes and the f_i are positive integers. Then

$$n = m^2 k = q_1^{2f_1} q_2^{2f_2} \cdots q_t^{2f_t} k.$$

This contradicts the fact that n is the product of distinct primes since, for example, q_1 appears more than once in the factorization for n. Therefore n is not divisible by any perfect squares.

(b) *Express the number* $32,955,000 = 2^3 \cdot 3 \cdot 5^4 \cdot 13^3$ *as the product of a squarefree number and a perfect square.*

Solution:

$$\begin{aligned} 32,955,000 &= 2^3 \cdot 3 \cdot 5^4 \cdot 13^3 \\ &= 2^2 \cdot 5^4 \cdot 13^2 \cdot 2 \cdot 3 \cdot 13 \\ &= (2 \cdot 5^2 \cdot 13)^2 \cdot (2 \cdot 3 \cdot 13) \\ &= 650^2 \cdot 78. \end{aligned}$$

Hence $32,955,000$ is the product of the perfect square 650^2 and the squarefree number $78 = 2 \cdot 3 \cdot 13$.

(c) *Let* $n \geq 2$ *be a positive integer. Then either* n *is squarefree, or* n *is a perfect square, or* n *is the product of a squarefree number and a perfect square.*

Solution: Let $n \geq 2$ be a positive integer. We factor n into primes using the fundamental theorem of arithmetic and break the proof into cases.

case 1: Suppose that n's prime factorization contains primes to even powers and primes to odd powers. Then

$$n = p_1^{2e_1} \cdot p_2^{2e_2} \cdots p_a^{2e_a} q_1^{2f_1+1} q_2^{2f_2+1} \cdots q_b^{2f_b+1}$$

where the p_i are the primes in the factorization of n that are raised to an even power and the q_i are the primes in the factorization of n that are raised to an odd power. We then have that

$$n = \left(p_1^{e_1} \cdot p_2^{e_2} \cdots p_a^{e_a} q_1^{f_1} q_2^{f_2} \cdots q_b^{f_b}\right)^2 q_1 \cdot q_2 \cdots q_b.$$

If all the e_i and f_i are zero then n is a squarefree number. Otherwise, n is the product of a perfect square and a squarefree number.

case 2: Suppose that n's prime factorization only contains primes to odd powers. Then

$$n = q_1^{2f_1+1} q_2^{2f_2+1} \cdots q_b^{2f_b+1}$$

where the q_i are primes. We then have that

$$n = \left(q_1^{f_1} q_2^{f_2} \cdots q_b^{f_b}\right)^2 q_1 \cdot q_2 \cdots q_b.$$

If not all the f_i are zero then n is the product of the perfect square and the squarefree number. If all the f_i are zero then

$$n = q_1 \cdot q_2 \cdots q_b$$

and so n is a squarefree integer.

case 3: Suppose that n's prime factorization only contains primes to even powers. Then there are primes p_i where

$$n = p_1^{2e_1} \cdot p_2^{2e_2} \cdots p_a^{2e_a} = \left(p_1^{e_1} \cdot p_2^{e_2} \cdots p_a^{e_a}\right)^2.$$

Here n is a perfect square.

9. Suppose that $x, y, z \in \mathbb{Z}$ such that $x > 0$, $y > 0$, $z > 0$, $\gcd(x, y, z) = 1$, and $x^2 + y^2 = z^2$. Prove that $\gcd(x, z) = 1$.

   Solution: Suppose that $x, y, z \in \mathbb{Z}$ such that $x > 0$, $y > 0$, $z > 0$, $\gcd(x, y, z) = 1$, and $x^2 + y^2 = z^2$. We now show that $\gcd(x, z) = 1$. We do this by showing that the negation of this cannot happen.

   Suppose that $\gcd(x, z) > 1$. Then, by exercise 5a, there exists a prime p such that $p|x$ and $p|z$. Then $x = pk$ and $z = pm$ for some integers k and m. Then $(pk)^2 + y^2 = (pm)^2$. Hence $p[pm^2 - pk^2] = y^2$. Thus $p|y^2$. Recall that if a prime divides a product of two integers then the prime must divide one of the integers. Therefore $p|y$. But then $p|x$, $p|y$, and $p|z$, which implies that $\gcd(x, y, z) \geq p$. This contradicts the fact that $\gcd(x, y, z) = 1$. Therefore, cannot have that $\gcd(x, z) > 1$.