Math 214 – Foundations of Mathematics
Homework 6

Due February 28, 2014

Alexander Powell

1. *(4 Points)*

   (a) Prove that $3|(n^3 - n)$ for every $n \in \mathbb{N}$;

   Solution:

   Proof. If $3|(n^3 - n)$ then there are 3 cases: $n = 3k$, $n = 3k$, and $n = 3k$.
   Case 1: $n = 3k$
   $((3k)^3 - (3k))$
   $= 27k^3 - 3k$
   $= 3(9k^3 - k)$
   So, $3|(n^3 - n)$ in this case.
   Case 2: $n = 3k + 1$
   $(3k + 1)^3 - (3k + 1)$
   $= 27k^3 + 27k^2 + 9k + 1 - 3k - 1$
   $= 3(9k^3 + 9k^2 + 3k - k)$
   So, $3|(n^3 - n)$ in this case.
   Case 3: $n = 3k + 2$
   $(3k + 2)^3 - (3k + 2)$
   $= 27k^3 + 54k^2 + 36k + 8 - 3k - 2$
   $= 3(9k^3 + 18k^2 + 12k - k + 2)$
   So, $3|(n^3 - n)$ in this case.
   Therefore, $3|(n^3 - n)$. □

   (b) In Homework 3.6, we have proved that $2|(n^3 - n)$ for every $n \in \mathbb{N}$. Use Theorem 11.16 and above results to prove $6|(n^3 - n)$ for every $n \in \mathbb{N}$.

   Solution:

   Proof. From theorem 11.16, if $a|c$ and $b|c$ then $(ab)|c$ if $gcd(a, b) = 1$. Since $2|(n^3 - n)$ from homework 3.6 and $3|(n^3 - n)$ from the above solution, and $gcd(2, 3) = 1$ then we can conclude that $(2 \cdot 3)|(n^3 - n)$ or $6|(n^3 - n)$. □

2. *(4 Points)* Suppose that $a, b, c \in \mathbb{N}$. Prove that $gcd(a, c) = gcd(b, c) = 1$ if and only if $gcd(ab, c) = 1$. (hint: Theorem 11.12: $gcd(a, b) = 1$ if and only if there exist $x, y \in \mathbb{Z}$ such that $ax + by = 1$).

   Solution:

Proof. This must be proven with two steps:

Step 1: We must prove that if $gcd(a,c) = gcd(b,c) = 1$ then $gcd(ab,c) = 1$. From theorem 11.12, $gcd(a,c) = 1$ iff $\exists x, y \in \mathbb{Z}$, such that:

$$ax + cy = 1$$

and

$$bw + cz = 1$$

Multiplying this out, we get:

$abxw = (1 - cy)(1 - cz)$

$abxw = 1 - c(y + Z - cyz)$

$c(y + Z - cyz) + abxw = 1$

Therefore, $gcd(ab,c) = 1$

Step 2: We must prove that if $gcd(ab,c) = 1$ then $gcd(a,c) = gcd(b,c) = 1$.

So, $\exists x, y \in \mathbb{Z}$ such that $abx + cy = 1$, which can be rewritten as:

$$b(ax) + cy = 1$$

Hence, there exist integer solutions to the equations $ax + cy = 1$ and $bw + cz = 1$. This implies that $gcd(a,c) = gcd(b,c) = 1$. □

3. *(4 Points)* Suppose that $a, b, c, d \in \mathbb{N}$, and $gcd(a,b) = d$. Prove that if $a|c$ and $b|c$, then $(ab)|(cd)$. (hint: use a similar proof as that of Theorem 11.16: since $d = ax + by$ for some $x, y \in \mathbb{Z}$, then $cd = c(ax + by)$)

   Solution:

   Proof. Since $gcd(a,b) = d$, then from theorem 11.12, $\exists x, y \in \mathbb{Z}$ such that

   $$ax + by = d$$

   Since $a|c$ and $b|c$, then $\exists d, e \in \mathbb{Z}$ such that $c = ad$ and $c = be$. From $ax + by = d$ we get

   $$acx + bcy = dc$$

   Substituting in the two equations for c above we get:

   $abex + bady = dc$

   $a(bex) + b(ady) = dc$

   $ab(ex + dy) = dc$

   So, we can conclude that $(ab)|(cd)$. □

4. *(4 Points)* (prove directly, and do not use Theorem 11.20)

   (a) Prove that $\sqrt{3}$ is irrational.

   Solution:

Proof. To prove that $\sqrt{3}$ is irrational we will use a proof by contradiction. Lets assume, to the contrary, that $\sqrt{3}$ is a rational number. Then $\sqrt{3}$ can be represented by the ratio $\frac{a}{b}$ where $a, b \in \mathbb{Z}$. So,
$3 = \frac{a^2}{b^2}$, or
$3b^2 = a^2$
Since $3|a^2$ and 3 is prime, then from 11.14, $3|a$ or $3|a$, thus $3|a$. Also, $b^2 = \frac{a^2}{3}$ so b^2 is divisible by 3, so $3|b$ or $3|b$, thus $3|b$. However, if a and b are both divisible by 3, that implies that they weren't in their lowest terms which is a contradtiction since we assumed that $gcd(a, b) = 1$. Hence, we have that $\sqrt{3}$ is irrational. $\square$

(b) Prove that $\sqrt{6}$ is irrational. (Hint: you can use results from Homework 4 and Result 5.15 and Theorem 5.16)

Solution:

Proof. Again, we will use a proof by contradition. First, assume that $\sqrt{6}$ is rational, so that it can be expressed as $\frac{a}{b}$, where $a, b \in \mathbb{Z}, b \neq 0$, and $gcd(a, b) = 1$.
Like we did above, we can get the equation $6b^2 = a^2$
$(2 \cdot 3)b^2 = a^2$
Since $3|a^2$ and 3 is prime, then $3|a$, so $\exists x \in \mathbb{Z}$ such that $a = 3x$. So, we have:
$(2 \cdot 3)b^2 = (3x)^2 = 9x^2$
$2b^2 = 3x^2$
Since $3|(2b^2)$ and $gcd(3, 2) = 1$ then from theorem 11.13 we get $3|b^2$ and since $3|b^2$ and 3 is prime then from 11.14 we know $3|b$. So, now we have found that $3|a$ and $3|b$ so 3 is a common divisor of a and b. Therefore, $gcd(a, b) \geq 3$ which contradicts with $gcd(a, b) = 1$. Hence $\sqrt{6}$ is irrational. $\square$

5. *(4 Points)* It is known from Theorem 11.20 that $\sqrt{k}$ is an irrational number if $k \in \mathbb{N}$ and $k \neq m^2$ for some $m \in \mathbb{N}$. Let $x \in \mathbb{R}$ and $x > 0$. Prove that there exists an irrational number between 0 and x. (hint: there are two cases: x is rational, or x is irrational)

Solution:

Proof. This will be a proof by cases: x is rational, or x is irrational.

Case 1: $x \in \mathbb{I}$ (Irrational)

If x is irrational, then the proof is simple:

Let $y = \frac{1}{2}x$, We know from Result 5.15 that an irrational number (x) multiplied by a rational number$(\frac{1}{2})$ is irrational. Therefore, y is an irrational number between 0 and x.

Case 2: $x \in \mathbb{Q}$ (Rational)

For the second case we can take a number like $\frac{\sqrt{2}}{2}$ which is between 0 and 1 and is irrational. Then there exists the number $y = \frac{\sqrt{2}}{2}x$ which is between 0 and x and makes y an irrational number. $\square$

6. *(4 Points)*

(a) Express each of the integers 4278 and 71929 as a product of primes (canonical factorization).

Solution: The canonical factorization of 4278 can be expressed as $1^1 \times 2^1 \times 3^1 \times 23^1 \times 31^1$, and the canonical factorization of 71929 can be expressed as $1^1 \times 11^1 \times 13^1 \times 503^1$.

(b) Find $gcd(4278, 71929)$ by using the canonical factorization.

Solution: Because the canonical factorizations of the two numbers share nothing in common except for 1, the $gcd(4278, 71929) = 1^1$ or 1.

7. *(extra 2 Points)* Prove that if p and q are prime numbers with $p \geq q \geq 5$, then $24|(p^2 - q^2)$.

8. *(extra 2 Points)* Let $n \in \mathbb{N}$ and let $n = \sum_{i=0}^{k} a_i \cdot 10^i$ be its decimal expression where $a_i \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Find a necessary and sufficient condition on $\{a_i\}$ so that $7|n$, and prove it. (Indeed problem 11.66 in textbook at least gives a special case, so you may generalize that one.)