First exam for Math 463

Prof. Bernardo Ábrego February 13, 2014.

Time limit: 75 minutes. Problems 1–5 are worth 20 points each, Problem 6 is worth 10 extra points. All your answers must be justified. Good luck!
In the following problems all variables are integers

1. Prove that $n^3 - n$ is divisible by 6 for every integer n.

   Solution 1. First note that $(-n)^3 - (-n) = -n^3 + n = -(n^3 - n)$. This we may assume that $n \geq 0$. Second, $n^3 - n = (n+1) \cdot n \cdot (n-1) = 6 \cdot \frac{1}{6}(n+1) \cdot n \cdot (n-1) = 6\binom{n}{3}$.

   Solution 2. If $3|n$, then $3|n(n^2-1) = n^3 - n$. If $3 \nmid n$, then $n = 3N \pm 1$ for some integer N. Thus $n^2 - 1 = (n-1)(n+1) = 3N(3N \mp 2)$, and it follows that $3|n(n^2-1) = n^3 - n$. Similarly, if $2|n$, then $2|n(n^2-1) = n^3 - n$. If $2 \nmid n$, then $n = 2K + 1$ for some integer K. Thus $n - 1 = 2K$ and it follows that $2|(n-1)(n+1) \cdot n = n^3 - n$. In all cases $2|n$ and $3|n$, so $6|n$.

2. Prove that $(a, a+2) = 1$ or 2 for every integer a.

   Note that $2 = 1 \cdot (a+2) + (-1) \cdot a$. Because $\gcd(a, a+2)$ divides every linear combination of a and $a+2$, it follows that $\gcd(a, a+2)|2$. The only positive divisors of 2 are 1 and 2, so $\gcd(a, a+2) = 1$ or 2.

3. Prove that $a|bc$ if and only if $\left.\frac{a}{(a,b)}\right| c$.

   Let $g = \gcd(a, b)$. Obviously $g|a$ and $g|b$, but also $\gcd(\frac{a}{g}, \frac{b}{g}) = 1$. Suppose $a|bc$, then $\frac{a}{g}|\left(\frac{b}{g}\right)c$. Because $\frac{a}{g}$ and $\frac{b}{g}$ are relatively prime, it follows that $\frac{a}{g}$ divides c. Conversely, suppose that $\frac{a}{g}$ divides c. Then $b \cdot \frac{a}{g}$ divides bc, however $\frac{b}{g}$ is an integer, so clearly a divides $a \cdot \frac{b}{g} = b \cdot \frac{a}{g}$, that in turn divides c. Therefore a divides bc.

4. Evaluate with proof (ab, p^4) and $(a+b, p^4)$ given that $(a, p^2) = p$ and $(b, p^3) = p^2$ where p is a prime.

   Let p^α and p^β be the largest powers of p that divide a and b, respectively. Because $\gcd(a, p^2) = p$ and $\gcd(b, p^3) = p^2$, it follows that $\min(\alpha, 2) = 1$ and $\min(\beta, 3) = 2$. Thus $\alpha = 1$ and $\beta = 2$. Therefore the largest power of p that divides ab is $\alpha + \beta = 3$, and $\gcd(ab, p^4) = p^{\min(3,4)} = p^3$. Similarly, the largest power of p that divides $a+b$ is p, because if p^2 were to divide $a+b$, then p^2 would divide $a + b + (-b) = a$, and the largest power that divides a is p. Therefore $\gcd(a+b, p^4) = p^{\min(1,4)} = p$.

5. Show that there exist non-negative integers x and y such that $x^2 - y^2 = n$ if and only if n is odd or is a multiple of 4. Show that there is exactly one such representation of n if and only if $n = 1, 4$, and odd prime, or four times a prime.

   Suppose that n is odd, then $x = \frac{1}{2}(n+1)$ and $\frac{1}{2}(n-1)$ are integers and

   $$x^2 - y^2 = (x+y)(x-y) = \left(\frac{1}{2}(n+1+n-1)\right)\left(\frac{1}{2}(n+1-n+1\right) = n.$$

   If n is a multiple of 4, say $n = 4N$ for some integer N, then let $x = N+1$ and $y = N-1$. Note that

   $$x^2 - y^2 = (x+y)(x-y) = (N+1+N-1)(N+1-N+1) = 2N \cdot 2 = n.$$

   Now suppose that $x^2 - y^2 = (x+y)(x-y) = n$ is even but not a multiple of 4. It follows that one of the factors $x+y$ or $x-y$ is even, and the other one is odd. But this is impossible, because their sum is equal to $x + y + x - y = 2x$, which is even.

   Suppose that n is odd but not equal to 1 or prime. Then $n = ab$ for some odd integers a and b with $1 < a \leq b < n$. Let $x = \frac{1}{2}(a+b)$ and $y = \frac{1}{2}(b-a)$. Note that both x and y are integers and

   $$x^2 - y^2 = (x+y)(x-y) = \left(\frac{1}{2}(a+b+b-a\right)\left(\frac{1}{2}(a+b-b+a\right) = ab = n.$$

Moreover this pair (x, y) is different from the solution pair $(\frac{1}{2}(n+1), \frac{1}{2}(n-1))$ shown before.

Suppose that n is a multiple of 4, $n = 4N$ for some integer N, but N is not equal to 1 or prime. Then $N = ab$ for some integers a and b with $1 < a \leq b < N$. Let $x = a + b$ and $y = b - a$. Note that

$$x^2 - y^2 = (x+y)(x-y) = (a+b+b-a)(a+b-b+a) = (2b)\cdot(2a) = 4ab = n.$$

Moreover this pair (x, y) is different from the solution pair $(N+1, N-1)$ shown before.

Finally, if n is equal to 1 or a prime, then n can only be written as a product of two positive integers as $1 \cdot n$. Thus we must have $x - y = 1$ and $x + y = n$, which yields the solution obtained before, and thus there is only one solution. Similarly, if $n = 4N$, where N is 1 or prime, then N can only be written as a product of two positive integers as $1 \cdot N$. If $n = (x+y)(x-y)$ is a multiple of 4, then given that $x + y + (x - y) = 2x$ is even, it follows that both factors must be even. The only way to write $n = 4N$ as a product of two even numbers is $2 \cdot 2N$, thus $x - y = 2$ and $x + y = 2N$ yields the only possible solution which was obtained before.

6. (Extra) Let a and b be positive integers such that $2 < b \leq a$. Prove that $2^b - 1$ does not divide $2^a + 1$.

   Suppose $2 < b \leq a$. Suppose that $a = bq + r$ where q and r are nonnegative integers such that $q \geq 1$ and $0 \leq r < b$. Performing long division yields

$$2^a + 1 = (2^b - 1)\left(2^{b(q-1)+r} + 2^{b(q-2)+r} + 2^{b(q-3)} + \cdots + 2^{b+r} + 2^r\right) + (2^r + 1).$$

   If $2^b - 1$ divides $2^a + 1$, then it follows that $2^b - 1$ divides $2^r + 1$. Thus $2^b - 1 \leq 2^r + 1$, but since $r < b$, it follows that $r \leq b - 1$ and then

$$2^b - 1 \leq 2^r + 1 \leq 2^{b-1} + 1.$$

   Thus $2^{b-1} - 1 \leq 2^{b-2}$. But $2^{b-1} - 1 = 1 + 2 + 2^2 + 2^3 + \cdots + 2^{b-2} > 2^{b-2}$ for $b > 2$, which is a contradiction. Thus $2^b - 1$ does not divide $2^a + 1$.